

ZiD-line

INFORMATIONEN DES ZENTRALEN INFORMATIKDIENSTES DER TU WIEN

Lenkungsausschuss

- Projektoffice
- Projektmanagement
- AG Technik
- Quantitätsmanagement
- Koordinationsausschuss
- Produktivsetzungsplanung
- Projektmarketing

TUWIS++ TU - INFO

Übersicht | Institute | Suche | Studienpläne | Hörsaalbelegung | Hilfe

Willkommen im TU Wien - Informationssystem (TUWIS++)

Auf diesen Seiten finden Sie Informationen über die Funktionen von TUWIS++ und die Eingabe Ihres Familiennamens. Sie werden dann nach Ihrem Namen sortiert.

Wenn Sie noch kein White Page als Studierende(r) an der TU Wien haben, können Sie dies hier eintragen.

Weitere Informationsangebote:
Mittelungsblätter der TU Wien
White Pages
Forschungsdokumentation
Publikationsdatenbanken

Design & Development: ADV/AB

TU-Passwort

TUWIS++ Informationssystem
SAP-Einführung an der TU Wien

Inhalt

Darf ich vorstellen: das TU-Passwort.	3
Das Informationssystem TUWIS++.	6
SAP-Einführung an der TU Wien	11
Open Source im öffentlichen Bereich	19
Itanium 2 und numerisch intensives Rechnen	21
Erste Windows 2003 Server Erfahrungen eines ungeschulten Administrators	26
Neue Firewall-Lösung für die TU-Institute auf Linux-Basis.	28
Wurmattaken	31
Internet-Service für Studierende: neue Räume und mobiler Zugang.	35
Auskünfte, Störungsmeldungen	38
Personalverzeichnis Telefonliste, E-Mail-Adressen	39

Impressum / Offenlegung gemäß § 25 Mediengesetz:

*Herausgeber, Medieninhaber:
Zentraler Informatikdienst
der Technischen Universität Wien
ISSN 1605-475X*

*Grundlegende Richtung: Mitteilungen des Zentralen
Informatikdienstes der Technischen Universität Wien*

Redaktion: Irmgard Husinsky

*Adresse: Technische Universität Wien,
Wiedner Hauptstraße 8-10, A-1040 Wien
Tel.: (01) 58801-42014, 42001
Fax: (01) 58801-42099
E-Mail: zidline@zid.tuwien.ac.at
www.zid.tuwien.ac.at/zidline/*

*Erstellt mit Corel Ventura
Druck: Grafisches Zentrum an der TU Wien,
1040 Wien, Tel.: (01) 5863316*

Editorial

Ein Hauptthema dieser Ausgabe der ZIDline ist die Einführung von SAP an der TU Wien, wobei der ZID an den intensiven Vorbereitungen beteiligt war und mit der ersten Tranche der Organisationseinheiten der TU Wien am 5. 1. 2004 mit SAP R/3 beginnen wird.

Um einen personalisierten Zugang zu Web-Applikationen zu ermöglichen, wird vermehrt das Passwort eingesetzt, das ursprünglich nur das Ändern von Daten in den White Pages erlaubte. Daher wurde es das „White Pages Passwort“ genannt. Aufgrund des Bedeutungswandels, den dieses Passwort vor allem in letzter Zeit erfahren hat, und der Verwirrung, die es manchmal hervorgerufen hat, nennen wir es ab sofort „TU-Passwort“. Wir hoffen, dass sich der neue Begriff bald etabliert.

Mit dem TU-Passwort gelangen Sie auch in das neue TUWIS++ Informationssystem, das eine zentrale Informationsquelle für den Universitätsbetrieb darstellt. TUWIS++ wird in einem eigenen Artikel ausführlich vorgestellt.

Der Ansturm der Studenten auf die Internet-Räume zu Semesterbeginn konnte rechtzeitig durch die Eröffnung der neuen Räume im renovierten ehemaligen Perlmöserhaus, Operngasse 11, bewältigt werden. 35 PCs und 8 Datentankstellen ergänzen das Angebot in unmittelbarer Nähe des Freihauses. Außerdem wurden die Bereiche am Campus, wo WLAN zur Verfügung steht, erweitert (siehe Plan auf Seite 37).

Weitere Themen dieser ZIDline sind Open Source, Benchmarks auf Itanium 2, Windows 2003 Server, Linux Firewall und die Wurmattaken der vergangenen Monate.

Das Titelbild zeigt – als grafischer Teil des Inhaltsverzeichnisses – im Hintergrund schematisch die WLAN-Bereiche am Campus und im Vordergrund einen neuen Internet-Raum im Perlmöserhaus, die TUWIS++ Einstiegseite und ein SAP Projektorganisationsdiagramm.

Ich bedanke mich sehr herzlich bei allen Autoren des ZID und allen Gastautoren für ihre Beiträge und die gute Zusammenarbeit.

Mit den besten Wünschen für 2004

Irmgard Husinsky

www.zid.tuwien.ac.at/zidline/

Darf ich vorstellen: das TU-Passwort

Zugang zu Web-Applikationen an der TU Wien

Irmgard Husinsky

Über Web-Anwendungen werden an der TU Wien immer mehr Informationen und Daten angeboten, siehe z. B. das neue Informationssystem TUWIS++. Zusätzlich zu den für die Allgemeinheit verfügbaren Daten können über persönliches Login Informationen und Dienste für bestimmte Personengruppen (Berechtigte) individuell zugänglich gemacht werden. Der Schlüssel zu diesen Informationsquellen ist das so genannte „TU-Passwort“.

Alle kennen die *White Pages*¹, das Personen- und Organisationsverzeichnis der TU Wien. Sie zeigen die dem tagesaktuellen Personalstand entsprechenden Daten und alle gültig rückgemeldeten Studierenden. Ferner können Institute weitere, nicht zum fixen Personal gehörige Personen dort aufscheinen lassen.

Allen diesen Personen steht ein Passwort zu, mit dem sie eine zunehmende Anzahl von Informationen und Diensten an der TU in Anspruch nehmen können. Dieses Passwort wurde bisher „White Pages Passwort“ genannt. Da dieser Begriff jedoch nicht mehr zutreffend ist und oft als verwirrend empfunden wurde, nennen wir es ab sofort „TU-Passwort“. Es ist der Schlüssel zu täglich benötigten Informationen für den Studien-, Lehr- und Forschungsbetrieb an der TU Wien sowie für Verwaltungsabläufe.

Über verschiedene Web-Applikationen an der TU Wien werden die Daten zur Verfügung gestellt. Da nicht jedem alle Informationen zugänglich sein sollen und außerdem die Informationen personalisiert werden können, muss beim individuellen Login in die Web-Anwendung überprüft werden, wer denn da Zutritt verlangt. Dies geschieht, indem der Nutzer einen Namen (Username,

Familiename etc.) und ein Passwort angibt. Dadurch soll sichergestellt werden, dass er auch berechtigt ist, bestimmte Daten einzusehen und bestimmte Dienste in Anspruch zu nehmen.

Die Überprüfung von Name und Passwort für die beschriebenen Web-Applikationen an der TU Wien erfolgt über die ZID Personendatenbank. Diese enthält die ZID-Kundendaten nicht nur aller TU-Angehörigen (Mitarbeiter im Personalstand und gültig rückgemeldete Studierende) sondern auch weiterer Personen (wie z. B. Drittmittelangestellte² und von Instituten eingetragene Personen). Jede Person kann nur ein einziges TU-Passwort haben, auch wenn sie mehrere Rollen in der Datenbank einnimmt (z. B. Mitarbeiter und Studierender).

Weitere Informationen über die ZID Personendatenbank und das Validierungsservice des ZID findet man in der ZIDline 7 [2].

Im Folgenden wird alles Wissenswerte über das TU-Passwort in Form von häufig gestellten Fragen (FAQ) angeführt.

¹ Der Begriff „White Pages“ („Weiße Seiten“) stammt aus dem englischen Sprachraum und steht für das eigentliche Telefonbuch, das in der Regel auf weißem Papier gedruckt ist (im Gegensatz zu den „Yellow Pages“, dem auf gelbem Papier gedruckten Firmenverzeichnis).

² Ab 1. 1. 2004 werden die bisherigen Drittmittelangestellten zu Angestellten des Unternehmens Technische Universität Wien und müssen dann nicht mehr separat eingetragen werden.

Welche Informationen und Dienste erschließt das TU-Passwort ?

- Personalisierter Zugang zum **TUWIS++ Informationssystem:**
für alle Mitarbeiter:
Lehrveranstaltungen (LVA) abonnieren, Terminkalender (auch private Termine), Listen für Arbeitsberichte, IBIS Verrechnungsinformation, Inventarinformationen, Kopierpapierbestellung, Drucksortenbestellung
für Vortragende zusätzlich:
LVA-Ankündigung, LVA-Abwicklung, LVA-Beauftragung (nur für Studiendekane), Rechtevergabe (nur für Supervisoren)
für Studierende:
LVAs abonnieren mit Forumsteilnahme, Stimmungszettel, LVA-Bewertung, persönlicher Terminkalender, Anzeigen von Prüfungen
für die Studienabteilung:
Sicht der Vortragenden, Hörsaalfreigabe
für alle, ohne Anmeldung:
Lehrveranstaltungsverzeichnis pro Institut, LVA-Suche, Studienpläne, Hörsaalbelegung
Siehe auch den Artikel über TUWIS++ auf Seite 6.
- **Benutzung der PCs in den Internet-Räumen** für Studierende. In den verschiedenen Gebäuden der TU Wien stehen in 12 Räumen über 220 Linux-Arbeitsplätze mit Internet-Zugang bereit.
- Für Studierende: **Beantragen von Kommunikationsdiensten:** TU-ADSL, VPN, WLAN, Inode xDSL, chello StudentConnect.
- Mitarbeiter der TU können **Benutzungsbewilligungen** für Services des ZID **online beantragen:**
Accounts auf zentralen Applikationsservern, Kommunikationsdienste (VPN- und Wählleitungszugang zum TUNET, Mobil-Zugang über Demo-Netz und WLAN),
E-Mail Accounts (zentrales Mailservice),
Kommunikationsdienste TU-ADSL, Inode xDSL, chello.
- Zugang zur **TUNET Datenbank** für Berechtigte.
- In die Personalliste (**White Pages** Darstellung) können **zusätzliche Informationen** eingetragen werden. Daten wie Name, Titel, Institutszugehörigkeit, Telefon, Raum und Funktion werden von der Zentralen Verwaltung vorgegeben. Zusätzliche E-Mail-Adressen, Telefone und Webadressen können von jeder Person selbst eingetragen werden.
- Diverse **Applikationen von Instituten**³:
Der ZID bietet allen Instituten der TU Wien die Möglich-

keit, das Validierungsservice für ihre Web-Applikationen zu verwenden. Zurzeit nutzen ein Chemie- und ein Architektur-Institut dieses Service für ihren Web-Zugang.

Wo bekomme ich das TU-Passwort ?

Studierende: Beim Einrichten eines Accounts für das Internet-Service (nach Vorlage des Studenausweises, bei den Studienassistenten im Internet-Raum FH1 oder bei den Operatoren des ZID) kann das Passwort gewählt werden. Berechtigt sind alle Studierenden, die an der TU Wien gültig rückgemeldet sind.⁴

Mitarbeiter der TU Wien: Mitarbeiter (im Personalstand der TU Wien) und so genannte „Weitere Mitarbeiter“ (vom Adressmanager eingetragene Personen) erhalten das TU-Passwort beim Adressmanager der jeweiligen Organisationseinheit.

Für die Zukunft ist ein besserer Mechanismus für die Verteilung des Passwortes an neue Mitarbeiter geplant.

Ich habe mein TU-Passwort vergessen

Studierende können bei den Studienassistenten (Internet-Raum FH1) oder bei den Operatoren des ZID (Freihaus, 2. Stock, roter Bereich) ein neues Passwort bekommen. Bitte unbedingt Studenausweis mitbringen.⁴

TU-Mitarbeiter können beim Adressmanager der Organisationseinheit ein neues Passwort gesetzt bekommen.

Wie kann ich mein TU-Passwort ändern ?

Das TU-Passwort kann über den Link „Daten ändern“ auf der White Pages Seite der entsprechenden Person geändert werden (whitepages.tuwien.ac.at).⁵

Nicht mehr oder noch nicht in den White Pages auftretende Personen können eventuell über die Maske „Nicht aktive Personen“ einsteigen: <https://iu.zid.tuwien.ac.at:8008/ZID-DB.editHiddenPerson>.

Studierende können das Passwort auch unter dieser Adresse ändern: <https://studman.ben.tuwien.ac.at/studacct/>.

Ich finde mich nicht in den White Pages

Die White Pages zeigen nicht alle in der ZID Personendatenbank gespeicherten Personen sondern den jeweils tagesaktuellen Personalstand. In der ZID Personendatenbank sind jedoch auch Personen vorhanden, die in vergangenen oder zukünftigen Semestern der TU angehört(en). Für diese gibt es einen Einstiegspunkt unter <https://iu.zid.tuwien.ac.at:8008/ZID-DB.editHiddenPerson>, wo auch das Passwort geändert werden kann.

³ Hinweis: Seit September 2003 steht das alte LDAP-Service unter wp.tuwien.ac.at („alte White Pages“) nicht mehr zur Validierung zur Verfügung.

⁴ Studierende, die auch im Personalstand der TU Wien sind, können ihr Passwort sowohl über die Studienassistenten als auch über den Adressmanager bekommen.

⁵ Zu beachten ist, dass dies nicht weltweit möglich ist, sondern nur von Rechnern innerhalb des TUNET bzw. von externen Zugängen zum TUNET (TU-ADSL, Wählleitungszugang, xDSL, chello StudentConnect und VPN).

Ferner ist zu beachten, dass die Suchfunktion in den White Pages nach Studierenden (nur gültig rückgemeldete) und Personal getrennt ist.

Wie lange gilt mein TU-Passwort ?

Wenn Sie aus dem Personalstand der TU Wien ausscheiden bzw. nicht mehr an der TU inskribieren, bleibt das TU-Passwort noch ein halbes Jahr gültig. So lange wird auch das Mail-Routing an die von Ihnen angegebenen Mailadressen durchgeführt.

Wer ist der für mich zuständige Adressmanager ?

Unter der Organisationseinheit, der Sie angehören, finden Sie in den White Pages bei den *Funktionen* unter „Adressmanager“ die entsprechende(n) Person(en), an die Sie sich wenden müssen.

Eine Liste der Adressmanager aller Organisationseinheiten der TU Wien findet man unter:
whitepages.tuwien.ac.at/suche/funktionen/adressmanager

Allgemeine Bemerkungen zum Umgang mit Passwörtern

Geschickte Auswahl und verantwortungsvoller Umgang mit dem Passwort schützen vor Missbrauch.

Das Passwort sollte nicht zu kurz sein, aber auch nicht zu lang (6 bis 8 Zeichen sollten von jeder Anwendung akzeptiert werden). Es sollte mindestens ein Zeichen enthalten, das kein Buchstabe ist.

Wählen Sie kein Passwort, das leicht zu erraten oder aus Ihren persönlichen Daten ableitbar ist.

Empfohlen wird, die Anfangsbuchstaben eines Satzes oder einzelne Silben aneinander zu reihen oder ein Wort mit Sonderzeichen oder Ziffern zu „spicken“.

Auch im Umgang mit dem Passwort sind einige Punkte zu berücksichtigen: nicht weitergeben, nicht aufschreiben, öfter wechseln, unbeobachtet eingeben.

Weiterführende Informationen

- [1] White Pages der TU Wien: whitepages.tuwien.ac.at
Online Dokumentation White Pages Service:
nic.tuwien.ac.at/services/white/
- [2] ZIDline 7, Oktober 2002,
G. Gollmann: ZID Personendatenbank,
J. Klasek: Pflege der Personen- und Institutsdaten,
J. Klasek: White Pages Service
www.zid.tuwien.ac.at/zidline/zl07/
- [3] ZID Validierungsservice:
macos.tuwien.ac.at/Authentifizierung.html
ZIDline 7, Oktober 2002:
www.zid.tuwien.ac.at/zidline/zl07/auth.html

Neues Service:

Online Account Management

Beantragen von Benutzungsbewilligungen über WWW

⇒ für Mitarbeiter der TU

⇒ Zugang mit dem TU-Passwort

⇒ kein Papierformular mehr ausfüllen

⇒ Bewilligungen für:

- Accounts auf den zentralen Applikationsservern
- E-Mail Accounts für zentrales Mailservice
- Accounts auf dem Informationsserver für Institute
- Berechtigung Wählleitungszugang zum TUNET
- Berechtigung VPN-Zugang zum TUNET
- Berechtigung Mobil-Zugang zum TUNET via Demo-Netz und WLAN

⇒ online Ändern, Verlängern, Löschen von Accounts

www.zid.tuwien.ac.at/zidaccounts.html

Das Informationssystem TUWIS++

Edmund Dvorak
Zentrale Verwaltung, ADV-Abteilung
edmund.dvorak@tuwien.ac.at

TUWIS++ (tuwis.tuwien.ac.at) ist die web-basierte und objektorientierte Erweiterung des seit vielen Jahren bestehenden Informationssystems TUWIS (www.tuwien.ac.at/ud/). TUWIS dient der Beschaffung, Sammlung, Aufschließung und Verbreitung von Informationen über den Lehr- und Studienbetrieb und der Information der Universitätsleitung sowie aller an der TU Wien interessierten Personen.

TUWIS ist eine Eigenentwicklung der ADV-Abteilung der Zentralen Verwaltung, verfügt über einen Datenbestand, der bis in das Jahr 1968 zurück reicht, und wird an der Technischen Universität Wien, an der Universität für Bodenkultur, an der Veterinärmedizinischen Universität und an der Universität für Musik und Darstellende Kunst eingesetzt. TUWIS basiert auf einer ORACLE-Datenbank, deren Datenmodell in den vielen Jahren seines Bestehens den jeweiligen Bedürfnissen der Fachabteilungen der Zentralen Verwaltung laufend angepasst worden ist. Die TUWIS++-Datenbank setzt auf dieser TUWIS-Datenbank auf und ermöglicht gemeinsam mit dem Zope-Programmsystem die Web-Anbindung von TUWIS.

Ziele von TUWIS++

Vorrangiges Ziel von TUWIS++ ist die Schaffung eines zentralen Web-Portals für alle Mitarbeiter, Vortragenden und Studierenden, das jedem anonymen Benutzer einen möglichst übersichtlichen Zugang auf alle offenen zugänglichen Informationen der TU Wien erlaubt. Dem authentifizierten Benutzer liefert es seine individuelle Sicht auf die zentral verfügbaren Daten in jener Form, wie er sie für seine tägliche Arbeit benötigt.

Ziel von TUWIS++ ist es auch, Verwaltungsabläufe klarzulegen, Papierversendungen so weit als möglich zu vermeiden und Unterschriften durch eine elektronische „Zustimmung“ zu ersetzen. Da die Übertragung dieser oft zahlungsrelevanten Informationen nicht nur im Intranet innerhalb der TU Wien möglich sein soll, sondern von jedem Rechner weltweit, ist nach dem Einloggen eine Verschlüsselung mit https vorgesehen.

TUWIS++ wird nach den Grundsätzen der höchstmöglichen Effizienz weiter ausgebaut. Unter „höchstmöglicher Effizienz“ verstehen wir das Verhältnis von Häufigkeit und Nutzen der möglichen Verwendung zum dafür notwendigen Entwicklungs- und Betreuungsaufwand. Das soll heißen, dass jene Dinge mit Priorität behandelt werden, die mit wenig Aufwand den größtmöglichen Nutzen versprechen.

Entwicklungskonzept

Um Zeit und Kosten zu sparen wurden in der Entwicklung die ausgezeichneten *Early Prototyping* Eigenschaften von Zope (c2.com/cgi/wiki?EarlyPrototyping) eingesetzt. Wir haben versucht, durch flexibles Software-Design TUWIS++ nach Bedarf und nach verfügbarer Entwicklungskapazität zu erweitern und zu verbessern. Dadurch wird es möglich, mehrfach geäußerte Verbesserungsvorschläge und Wünsche der Anwender einfacher und rascher zu realisieren.

TUWIS++ soll leben und Leben ist Veränderung. So wird bewusst in Kauf genommen, dass sich bestimmte, bereits gewohnte Menüstrukturen ändern können und bestimmte Informationen an anderer Stelle auftauchen. Wir sind überzeugt, niemand ist unfehlbar und allwissend und auch bei jeder noch so vollständigen und langfristigen Planung hätte es jede Menge an Veränderungen geben müssen. Gerade im Jahre 2003, mit den gravierendsten Veränderungen an den Universitäten seit Beginn des EDV-Einsatzes (Vollrechtsfähigkeit, neue Fakultätengliederung, SAP-Einsatz), erscheint uns das der richtige und eigentlich der einzig mögliche Ansatz.

TUWIS++ Hörsaaltermine							TU	
Übersicht Institute Suche Studienpläne Hörsaalbelegung Hilfe							TU WIEN	
Tuwis++: <input type="text"/>							login	
							Englisch	
<< 11.2003 >>								
Mo	Di	Mi	Do	Fr	Sa	So		
						07:00		07:00
						07:30		07:30
						08:00		08:00
						08:30		08:30
						09:00		09:00
						09:30		09:30
						10:00		10:00
						10:30		10:30
						11:00		11:00
						11:30		11:30
						12:00		12:00
						12:30		12:30
						13:00		13:00
						13:30		13:30

Mo	Di	Mi	Do	Fr	Sa	So
		07:30 - 08:30 188.207 - Einführung in die Informatik (EI 7 Hörsaal)				
				08:15 - 12:00 360.016 - Programmieren 1 (EI 7 Hörsaal)		
09:15 - 10:00 101.132 - Mathematik 1 f. ET (EI 7 Hörsaal)	09:15 - 10:00 101.132 - Mathematik 1 f. ET (EI 7 Hörsaal)	09:15 - 10:00 101.132 - Mathematik 1 f. ET (EI 7 Hörsaal)	09:15 - 10:00 101.132 - Mathematik 1 f. ET (EI 7 Hörsaal)			
10:15 - 11:00 351.008 - Elektrotechnik 1 (EI 7 Hörsaal)	10:15 - 11:00 351.008 - Elektrotechnik 1 (EI 7 Hörsaal)	10:15 - 11:00 351.008 - Elektrotechnik 1 (EI 7 Hörsaal)	10:15 - 11:45 175.033 - Wirtschaftswissenschaften 1 (EI 7 Hörsaal)			
11:00 - 13:00 184.166 - Verteilte Systeme (EI 7 Hörsaal)	11:00 - 12:30 258.001 - Zeichnen und visuelle Sprachen (Teil 1) (EI 7 Hörsaal)	11:00 - 13:00 184.166 - Verteilte Systeme (EI 7 Hörsaal)				
12:00 - 14:00 102.437 - Repetitorium Math.I f. MB und BI (EI 7 Hörsaal)						
13:00 - 20:00 Dr. Schönhuber Prf		13:00 - 20:00 E351 Schönhuber	12:15 - 13:45 175.034 - Wirtschaftswissenschaften Übungen (EI 7 Hörsaal)			

Beispiel: Hörsaalbelegung EI 7, Anfang November 2003

Die technische Entwicklung mit dem Verfall der Hardwarepreise und der weltweiten Verfügbarkeit der gleichen Programme auf allen Plattformen ermöglicht allen Mitarbeitern und Studierenden zu relativ geringen Kosten einen Zugang zu einem zentralen Datenbestand, ohne Rücksicht auf Standort und eingesetzte Hardware.

Häufig auftretende Verwaltungsvorgänge, die schon bisher in traditioneller Weise mit Formularen abgewickelt worden sind, werden als Web-Formulare angeboten, vom eingeloggten Antragsteller ausgefüllt und an die zuständige Fachabteilung elektronisch weitergeleitet, wobei jede involvierte Stelle den Ablauf (*Workflow*) verfolgen und die Daten sofort am Ort der Entstehung ergänzen kann. Jedes Ausfüllen von Papierformularen bzw. jeder Ausdruck von ausgefüllten Formularen führt zwangsweise zu Doppelarbeit, wenn die Daten weiter verarbeitet werden sollen. Unabhängig vom manipulativen Aufwand und vom Zeitverlust beim Versand entsteht vor allem durch fehlerhafte oder unvollständige Anträge auf Papier beträchtliche Mehrarbeit für die Ausfüllenden und für die Fachabteilung („Papier ist geduldig“).

Alle Zugriffsrechte in TUWIS++ sind in Rollen zusammengefasst und an beliebig definierbare Personengruppen delegierbar. Berechtigte Benutzer können jede ihrer Rollen bei Bedarf an Personen ihres Vertrauens weitergeben und, sollte dieser Bedarf nicht mehr gegeben sein, auch diesen Personen wieder entziehen. Es gibt daher keine Notwendigkeit, mit Zustimmung des Inhabers einer Rolle unter „falschem Namen“ zu arbeiten.

Dies kann immer wieder zu Missverständnissen und Verwirrung führen und erschwert außerdem die Fehlersuche oft enorm.

Datenqualität

Die weite Verbreitung des Internets ist als Chance für die Verbesserung der Datenqualität zentraler Datenbestände zu sehen. Nur wenn alle Betroffenen ihre individuelle Sicht auf die Daten erhalten und diese auch wahrnehmen, wird es möglich sein, die Daten laufend zu aktualisieren, zu vervollständigen und die Datenqualität zu verbessern. Nicht laufend in Verwendung befindliche Daten entwickeln sich recht rasch zu „Datenfriedhöfen“ ohne praktischen Nutzen. Eine hohe Datenqualität ist aber die Voraussetzung für die Akzeptanz des ganzen Systems und damit für den effizienten Ablauf der Verwaltungsvorgänge.

Nicht der Zwang zur Verwendung eines Informationssystems kann dessen Verbreitung sichern, sondern nur der Nutzen für jede individuelle Benutzergruppe.

So ist immer zwischen Erhebungsaufwand und potentielltem Nutzen abzuwägen, bevor neue Daten von Benutzern eingefordert werden dürfen. Der Bedarf an Daten ist fast immer von jenen gegeben, die mit der Erhebung nichts zu tun haben wollen – aber die Lust und Zeit zum Erheben und Einfordern dieser Daten ist naturgemäß sehr gering.

Nur wenn die Vorteile für jene, die die Daten liefern sollen, überwiegen, werden sie bereit sein, ihre wertvolle Zeit für die Datenerhebung zur Verfügung zu stellen, und nur wenn die Datenverantwortlichen die Möglichkeit haben, mit ihren Daten selbst zu arbeiten, werden sie auf Aktualität und Vollständigkeit achten.

Lehrangebot pro Person / Beauftragung durch den Studiendekan

Zurück

Thomas Mustermann Ass.Prof. Dipl.-Ing. Dr.techn.

Semester: 2003W

B	Nr.	Std.	Stunden	Typ	Block	Titel	Art	Anm.	Fakt./ Venia	Prüfungszahlen			
										01W	02S	02W	03S
<input type="checkbox"/>	382.012	3.00	1.00	SE		Research Projects in Advanced Signal Processing	selb.Ass		0.50				
<input checked="" type="checkbox"/>	382.624	3.00	2.00	SE		Digitale Signalverarbeitung A	selb.Ass		0.50	10	7		Lehrzulage
<input checked="" type="checkbox"/>	382.646	1.50	1.50	VO		Signalprozessoren	selb.Ass		1.00	32	34		LZ +345,35
<input checked="" type="checkbox"/>	389.001	3.00	3.00	LU		Signalverarbeitung mit Matlab	selb.Ass		0.50	3	6		1036.05
<input checked="" type="checkbox"/>	389.065	2.50	2.50	VU		Signalprozessoren	selb.Ass		0.50				863.38
<input checked="" type="checkbox"/>	389.092	9.00	2.80	LU		Nachrichtentechniklabor B	selb.Ass		0.50	6	18		966.98

Abteilung für dieses Semester: als Assistent Lehrzulage für 2.0 Stunden **2179.10**
als Assistent für selbständige Abhaltung 4.65 Stunden à 690.70 **3211.76**
Gesamt 5390.86

Beispiel: Beauftragung Lehrangebot

Zentrale Web-Services an der TU Wien

In den letzten Jahren hat sich eine fast unüberschaubare Fülle von verschiedenen zentralen, web-basierten Informationssystemen an der TU Wien (HISTU, LZK, SIDES, SIDES-4mi, White Pages, SW-Lizenzen, Publikationsdatenbank, FoDok, Web-Mail usw.) entwickelt, von ganz unterschiedlichen Organisationseinheiten betreut, deren „Harmonisierung“ dem neuen (und alten) Rektor und seinem Rektorat ein großes Anliegen ist.

An der TU Graz wird bereits seit sechs Jahren mit enormem personellem und finanziellem Aufwand ein wirklich beeindruckendes Informationssystem TUG-Online (https://online.tu-graz.ac.at/tug_online/webnav.ini) aufgebaut, das zu Recht nationale und internationale Anerkennung erlangt hat. Die TU Wien wird versuchen, mit wesentlich bescheideneren Mitteln ein auf ihre Bedürfnisse zugeschnittenes einheitliches Informationssystem zu entwickeln, das im Ansatz wohl mit TUG-Online vergleichbar sein soll (eine zentrale Datenbasis, Zugriff für alle Mitarbeiter und Studierenden, Transparenz der Daten und Abläufe, *SingleSignOn*), in der Realisierung aber moderner und herstellerunabhängig (Open-Source, objekt-orientierte Datenbank, integriertes CMS) und mit wesentlich geringeren Hardware-Ressourcen (Zope-Cluster, *Load Balancing*) auskommen soll. Angelehnt an das von der PR-Abteilung entwickelte Corporate Design der TU Wien, über Style-Sheets jederzeit änderbar, soll das Layout an die statischen Seiten der Verwaltung (www.tuwien.ac.at/zv/) angepasst sein und die Basis für einen einheitlichen Web-Auftritt des Unternehmens darstellen.

(Kurze) Entwicklungsgeschichte

Die Geschichte von TUWIS++ ist noch sehr kurz: Nach den gescheiterten Vertragsverhandlungen mit der TU Graz über die Mitverwendung von TUG-Online wurde am 8. 4. 2003 dem Vizerektor für Lehre und den Studiendekanen von Dipl.-Ing. Felix Beer ein Prototyp eines „Lehrveranstaltungs-Erfassungs- und -Beauftragungssystems“ (LVPLAN) vorgestellt, das nicht nur ein vollständiger Ersatz des in Ungnade gefallenen SIDES LVA-Editors war, sondern zusätzlich noch die Möglichkeit der Neuanündigung von Lehrveranstaltungen (LVAs) inklusive der Reservierung von Hörsaalterminen beinhaltete und allen Vortragenden einen *Workflow* zeigte, wo jederzeit der Ankündigungszustand der LVA abgelesen werden konnte. Die LVA-Ankündigung ging als erste TUWIS++-Applikation noch im Mai in den Echtbetrieb – für die Komplexität der Aufgabenstellung eine, wie wir glauben, sensationell kurze Entwicklungszeit.

Als nächster Schritt, und nach den Erfahrungen der erfolgreichen LVA-Erhebung für das laufende Studienjahr mutig geworden, erfolgte durch Vizerektor Schimak nicht zuletzt aus Gründen des hinreichend bekannten Sparbudgets von 2003 – die Neuentwicklung von TUWIS++ kam der TU ganz wesentlich billiger als der laufende Betrieb der dadurch abgelösten Systeme – der Auftrag zur Schaffung eines Ersatzsystems für den Lehrzielkatalog (LZK) und SIDES-4mi. Das System sollte unter Anleitung und Mitarbeit von Dipl.-Ing. Felix Beer von der ADV-Abteilung entwickelt und betrieben werden. Zwar nicht ganz im geplanten Funktionsumfang, aber rechtzeitig zum 1. 9. 2003 war damit die eigentliche „Geburts-

stunde“ von TUWIS++ gegeben, als offenes LVA-Informationssystem mit Studienplänen, Anzeige der Organisationseinheiten und deren Vortragenden und einer grafischen Stundenplandarstellung von Hörsälen und Seminarräumen, aber auch als Basis eines vollständigen Informationssystems für Mitarbeiter, Vortragende und Studierende mit Authentifizierung mittels des TU-Passworts.

Geplante Erweiterungen

Als nächster Schritt ist die Ausweitung von TUWIS++ vom Schwerpunkt LVAs auf „Allgemeine Informationen“ vorgesehen, wobei über

- Organisationseinheiten und Personen,
- Studium und Lehre (Studienpläne, LVAs, Prüfungs-Anmeldung),
- Forschung (Projekte, Publikationen),
- Objekte (Hauptstandorte, Gebäude, Räume, Pläne),
- Dokumente (Mitteilungen, Mitteilungsblätter, Formulare),
- Statistiken (Zahlen, Daten, Fakten)

Informationen geliefert werden sollen.

Welche Applikationen im Einzelnen als „besonders wichtig“ eingestuft werden und daher früher begonnen werden, ist noch nicht entschieden. Nach den bereits im Echtbetrieb befindlichen Applikationen

- Ankündigung und Beauftragung der Lehre,
- Hörsaalreservierungen durch Vortragende,
- Ersatz von SIDES-4mi (Abonnieren von LVAs, Evaluierung der Lehre)

wären sicher wünschenswert:

- Web-basierte Prüfungsanmeldung,
- Unterstützung von Gruppenbildung bei der Anmeldung zu Lehrveranstaltungen,
- Verbesserung der LVA-Bewertung durch gruppenbezogene Bewertungsmöglichkeiten,
- Vollständige Studienplan-Zuordnung von Lehrveranstaltungen, danach automationsunterstützte Ausstellung von Diplomprüfungszeugnissen,
- Zusammenführung und Verbesserung der Applikationen FoDok, Publikationsdatenbank und Aufbau einer Drittmittel-Projekt-Datenbank,
- Darstellung aller laufenden und geplanten Bauprojekte im Web,
- Rollenkonzept zur Versendung von Massen-E-Mails,
- Verbesserung der Funktionalität der einzelnen Abläufe durch *Workflow*-Systeme (Reisekostenanträge und Freistellungen, Aktenablage – nicht nur Registrierung, Urlaubsbewilligungen),
- „Selbstbedienung“ für Studierende (Zeugnis- und Bestätigungsdruck, Ändern der Adressen, SB-Terminals in der Aula),
- Facility-Management zur einfacheren Gebäudeverwaltung,
- *Data Warehouse* für einfacheren Zugang zu Datenauswertungen,
- Management-Informationssystem (MIS).

Eingesetzte Software

TUWIS++ ist in Zope (www.zope.org) realisiert. Zope ist ein *Open-Source*-Webanwendungs-Server und unterstützt Arbeitsgruppen beim Erstellen und Verwalten von dynamischen web-basierten Geschäftsanwendungen wie Intranets und Portalen. Er wird von der Zope-Corporation (www.zope.com) laufend weiter entwickelt, läuft auf praktisch allen UNIX- und NT-Plattformen und kann mit dem eigenen, integrierten Web-Server oder jedem beliebigen anderen (in unserem Fall: Apache) eingesetzt werden.

Zope ist in Python (www.python.org) geschrieben, einer mächtigen, objektorientierten Programmiersprache, die mit der steigenden Beliebtheit von Google stark an Bekanntheit gewonnen hat, weil große Teile von Google in Python geschrieben sind. Die in Zope integrierte, auf Transaktionen basierende, objektorientierte Datenbank kann nicht nur Daten und Programmcode speichern, sondern auch dynamische HTML-Templates und ausführbare Scripts, enthält eine interne Suchmaschine und kann Verbindungen zu unterschiedlichen relationalen Datenbanken herstellen.

Programme in Zope können in verschiedenen Programmiersprachen entwickelt werden, allen voran natürlich Python, DTML, Page Templates, aber auch z. B. Perl wäre möglich.

Das in Zope enthaltene, höchst komplexe und vielfältige Sicherheits-Modell erlaubt die sichere Delegation von Rollen und Rechten und damit die Entwicklung von Zope-Objekten oder Applikationen direkt im Web-Browser von überall in der Welt.

Eine fast unüberschaubare Menge von *Zope-Plug-Ins* ist als *Open-Source* im Internet verfügbar und ermöglicht eine individuelle Konfiguration der eigenen Entwicklungsumgebung nach den persönlichen Bedürfnissen. Der Bogen reicht von kompletten *e-Commerce*-Applikationen über Content- und Dokumenten-Managementsysteme, *Workflow*-Systeme und *Caching*-Algorithmen bis zum *Load-Balancing* bei Großanwendungen. Die weltweit sehr aktive Zope-Community kann für jedes Problem verschiedenste Lösungen anbieten – Interessenten finden z. B. auf der *Site* der Deutschen Zope User Group (www.dzug.org) eine Fülle von weiteren Informationen.

Technische Realisierung

Bei der Realisierung von TUWIS++ konnte auf den *Source Code* des Pilotsystems LVPLAN und des ein Jahr zuvor an der Universität für Bodenkultur entstandenen BLIS (Boku Lehre-Informationssystem) zurückgegriffen werden.

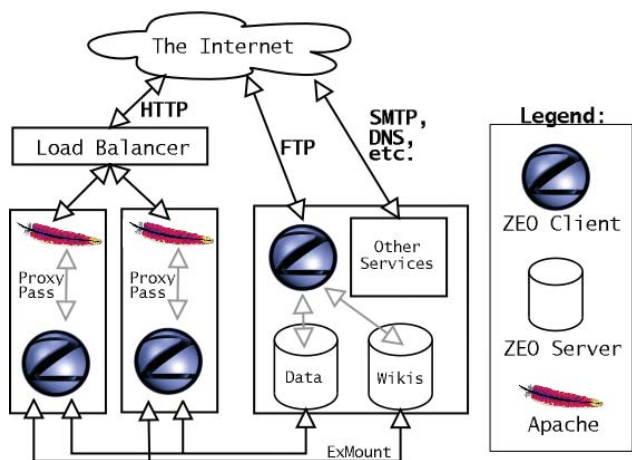
Obwohl diese Systeme auf unterschiedlicher Hardware, mit unterschiedlichen Betriebssystemen und unterschiedlichen Datenbanken eingesetzt wurden, fiel der Aufwand zur Portierung sehr gering aus.

BLIS arbeitet auf einem Dual-Pentium-III System (2x 1.26 GHz, 1 GB RAM, SCSI) mit SuSE-Linux und PostgreSQL-Datenbank, LVPLAN wurde auf einer SUN (2x 600 MHz, 600 MB RAM, SCSI) unter Solaris und Oracle 8i eingesetzt und TUWIS++ schließlich läuft auf einem

Dual-Xeon-Rechner mit Hyperthreading (2x 2.4 GHz, 2 GB RAM, SCSI) und RedHat-Linux Advanced Server auf Oracle 9i.

Als Entwicklungsplattform für TUVIS++ wird ein PC (Athlon 800 MHz, 256 MB RAM, IDE) unter Gentoo Linux mit Oracle 8i eingesetzt, der von bis zu vier Entwicklern gleichzeitig verwendet wird.

Anfängliche Befürchtungen, Zope als Plattform könnte dem Ansturm möglicherweise nicht gewachsen sein, haben sich inzwischen zerstreut, und auch für zukünftige Herausforderungen ist ausreichend Spielraum vorhanden – sollte irgendwann ein Server nicht mehr ausreichen, könnte über ZEO eine skalierbare Clusterlösung geschaffen werden.



Zope Cluster

Entwicklungsumgebung

Für die Entwicklung einer Zope-Anwendung wird normalerweise nicht mehr benötigt als ein Zope-Server und ein installierter Web-Browser.

Die Programmentwicklung kann komplett über den Browser abgewickelt werden, spezielle Entwicklungswerkzeuge sind in der Regel nicht nötig. TUVIS++ wurde vorwiegend in DTML und Python entwickelt.

Das Zusatzprodukt „externalEditor“ gestattet die Einbindung der Lieblings-(Programm-/Bild-/Web-)Editoren des jeweiligen Entwicklers, wenn dieser das wünscht.

SingleSignOn, SingleLogin

Eine wesentliche Anforderung an TUVIS++ war die Notwendigkeit, die Benutzeranmeldung (Authentifizierung) über das TU-Passwort zu realisieren, weil zum einen der LDAP-Dienst im Auslaufen begriffen ist und andererseits eine eigene Benutzerverwaltung aufwendig zu pflegen, für die Benutzer unbequem (Passwortänderung) und darüber hinaus unsinnig wäre.

Die Authentifizierung von Benutzern ist in Zope über so genannte „User Folder“ realisiert, die in verschiedenen Ausprägungen verfügbar sind. Ein besonders interessantes und flexibles Produkt ist der „extensible User Folder“ (XUF), der sich durch leichte Erweiterbarkeit und austauschbare (wenn auch nicht beliebig kombinierbare) Authentifizierungs- und Property-Verwaltungs-Module auszeichnet.

Dieser Folder wurde an die an der TU herrschenden Verhältnisse angepasst und regelt sowohl die Anmeldung als auch die Vergabe der Rollen an die Benutzer.

Unter *SingleSignOn* versteht man den Versuch, alle verwendeten Web-Applikationen (Programme) so zusammenzuschalten, dass nur eine einzige Anmeldung des Benutzers nötig ist, unter *SingleLogin* einfach den Umstand, dass ein und derselbe Benutzer alle Programme mit demselben Benutzernamen / Passwort-Kombination benutzen kann, dieses aber womöglich beim Wechsel von einem Programm zum anderen extra eingeben muss.

Dem verständlichen Wunsch des Rektors nach einer integrierten Lösung Rechnung tragend wurden die bislang schon von der ADV-Abteilung gewarteten Programme mit TUVIS++ soweit integriert, dass keine neuerliche Anmeldung vonnöten ist.

Datenbankanbindung

Die Anbindung an die Datenbanken erfolgt über „Datenbankadapter“, der eigentliche Zugriff auf die Daten über „Queries“ (Abfragen), wobei einem Query ein Datenbankadapter zugeordnet wird. Durch Tauschen des Adapters kann ein Programm im Idealfall ohne weitere Anpassungen an eine neue Datenbank gebunden werden. Innerhalb von Zope können mehrere Datenbankadaptern gleichzeitig verwendet werden.

Die Anbindung an die TUVIS++-Datenbank erfolgt über den Datenbankadapter „DCOracle2“, Connection-Pooling und Transaction-Handling wird von Zope selbst beigesteuert.

Zukunftsansichten von TUVIS++

Wiewohl ein neues System und das zwangsweise Verlassen einer gewohnten Umgebung eher zu Kritik als zu Lob ermutigen, haben die Anwender TUVIS++ recht positiv aufgenommen. Neben durchwegs konstruktiver Kritik haben die positiven Meinungen bei weitem überwogen und gerade am Anfang, als viele Funktionen noch nicht optimal gelaufen sind, hat uns das vielfach erhaltene Lob gezeigt, dass wir auf dem richtigen Weg sind.

Wir stehen selbstverständlich auch Ihnen für Anregungen, Wünsche, Beschwerden und Fragen unter tuwis@zv.tuwien.ac.at zur Verfügung und bemühen uns, im Rahmen unserer Kapazitäten so schnell wie möglich darauf zu reagieren.

SAP-Einführung an der TU Wien

Es wird ernst – kurze Geschichte und einige technische Aspekte des Projekts „uni.verse“

Wolfgang Kleinert

Die Technische Universität Wien wird ab 1. 1. 2004 gemäß UG 2002 und Rechnungslegungsverordnung des BMBWK so wie auch alle anderen 20 vollrechtsfähigen Universitäten Bilanzen erstellen und ein dem ersten Abschnitt des dritten Buchs des Handelsgesetzbuchs entsprechendes Rechnungswesen führen müssen. Am 5. 1. 2004 geht das IT-Verfahren „uni.verse“ für das neue Rechnungswesen in den Echtbetrieb.

Die Zeiten des Bundeshaushaltsgesetzes (BHG) und der entsprechenden IT-Verfahren (HV, HV-online, BVI, IBIS) werden auch für die TU Wien mit Jahresende 2003 vorüber sein. Die Institute wurden und werden bereits vom Rektorat durch Veranstaltungen und andere Informationen ausführlich auf die neue Situation vorbereitet. Hier soll ein wenig die Geschichte der geplanten SAP-Einführung erzählt und einige technische Aspekte des neuen IT-Verfahrens sowie die Anforderungen an die Hard- und Software auf Seiten der Institute (Clients) beleuchtet werden.

Vorgeschichte

Im Juni 2002 hat das BMBWK in Erweiterung des bereits seit mehreren Jahren laufenden Projektauftrags „HV-SAP“ (d.h. die Umstellung der Applikation „Haushaltsverrechnung des Bundes“ auf SAP R/3, mit dem Auftraggeber BMF, dem Generalunternehmer Siemens Business Services (SBS) und dem Betreiber Bundesrechenzentrum GmbH (BRZ)) der Firma SBS den Auftrag erteilt, als Generalunternehmer und Projektleiter „... das abschnittsweise Redesign des Rechnungswesens gemäß UG 2002 der Universitäten unter Heranziehung der Standardsoftware SAP R/3“ durchzuführen und den Echtbetrieb durch das BRZ vorzubereiten. Mögliche Alternativen wurden wegen des großen Zeitdrucks bei der Implementierung des UG 2002 offensichtlich nicht ernsthaft in Erwägung gezogen. Eckdaten dieses Auftrags waren u.a.:

- der „Einsatz der betriebswirtschaftlichen Standardsoftware R/3 der Firma SAP in allen 21 Universitäten in der vereinbarten Funktionalität“, das sind die Module FI, FI AA, FI FM, CO, PS, MM, SD, BW (diese Kürzel stehen für Finanzbuchhaltung, Anlagenbuchhaltung, Fondsmanagement=Budgetverwaltung, Kostenrechnung, Projektssystem, Materialwirtschaft inkl. Bestellwesen, Vertrieb inkl. Fakturierung und Business Warehouse)
- die „weitestgehende Beschränkung auf den SAP-Standard“
- die „Schaffung eines benutzerfreundlichen, ergonomischen IT-Verfahrens „UNI-SAP“, welches bei den Anwendern auf hohe Akzeptanz stößt“
- „ein möglichst problemloses Zusammenspiel von UNI-SAP mit den IT-Anwendungen der Universitäten“
- ein „Go Live“ am 1. 1. 2004

(alle Zitate aus der „Projektpräsentation Kick-off Baden“ vom 24. 9. 2002, zu finden auf der Projekt Homepage [1], siehe auch die gute Zusammenstellung der Universität Innsbruck [2]).

„UNI-SAP“ wurde inzwischen in „uni.verse“ umbenannt. Bis zum 1. 1. 2005 soll dann auch das auf dem SAP-Modul HR (steht für Personalmanagement und -verwaltung) beruhende IT-Verfahren „uni.pers“ die Altapplikation „Besoldung“ im BRZ abgelöst haben. An diesem Verfahren werden 16 Universitäten (darunter auch die TU Wien) teilnehmen und damit die Lohnverrechnung und Gehaltsauszahlung durchführen. Für das Jahr 2004 wird die Altapplikation „Besoldung“ (PIS, PAV) auch

für die Drittmittelangestellten weiterlaufen. Nach dem UG 2002 bleiben nur mehr die Beamten auch in Zukunft in der Bundesbesoldung, die ebenfalls mit 1. 1. 2005 auf SAP HR umgestellt werden soll (Projekt „PM-SAP“).

SAP R/3 - was ist das ?	
Was verbirgt sich hinter dem Kürzel SAP ?	
Bedeutung:	Quelle:
Systeme, Anwendungen, Produkte in der Datenverarbeitung	SAPGUI Ver. 3.0 f
Ursprünglicher Name (1972): Systemanalyse und Programmentwicklung	SAP AG
Fehlinterpretationen:	
Software, Anwendungen und Probleme	Prof., anonym
Submit and pray	Anonymus
Was verbirgt sich hinter dem Kürzel R/3?	
Bedeutung:	Quelle:
R: realtime-processing - Echtzeitverarbeitung	webmaster@sap-ag.de
3: Dreistufige Client/Server-Architektur	
www.fh-brandenburg.de/~sap_r3/info/w_sap.htm	

Ich erinnere mich noch gut an meine Probleme mit der SAP-Terminologie. Selbstverständlich braucht jede technische Disziplin eigene Begriffe um Sachverhalte effektiv zu beschreiben, die sich von der Begriffswelt anderer Disziplinen unterscheiden, eben einen eigenen Wortschatz (und dieser Artikel ist selbst ein anschauliches Beispiel dafür). Daher hat bei mir z. B. ein Satz wie: „Für die Realisierung des Cut-over-Plans müssen die Change Requests für das Rollout der zweiten Tranche bis zum x. x. 2003 abgenommen werden“ zwar zunächst völliges Unverständnis hervorgerufen, aber gleichzeitig meine Neugier erweckt, die Definition der mir unbekannt Begriffe zu erforschen. Größere Schwierigkeiten hatte ich immer mit Aussagen wie: „Für die detaillierte Kostenverfolgung müssen statistische Innenaufträge angelegt werden“. Das klingt zunächst wie ein ganz normaler Satz und doch erweckt er keinerlei brauchbare Assoziationen. Dieses Kauderwelsch, das natürlich den SAP-Gurus und -Beratern flüssig von den Lippen kommt, erschwert es dem SAP-Novizen ohne betriebswirtschaftliche Vorbildung, das unglaublich mächtige betriebswirtschaftliche Werkzeug auf Anhieb zu verstehen.

Das Vorhaben, innerhalb von 18 Monaten 21 Unternehmen auf SAP R/3 umzustellen und gleichzeitig völlig neue Rahmenbedingungen für das Rechnungswesen einzuführen, war gelinde gesagt äußerst ambitioniert. Es gibt weltweit dafür kein Referenzmodell. Die TU München hat z. B. für ihre SAP-Einführung einen Zeitraum von 30 Monaten geplant (siehe auch den nett geschriebenen Newsletter „SAPalott“ [3]). Der Ansatz des Generalunternehmers bestand daher in der ziemlich strikten Anwendung der Standardempfehlungen von SAP für die

Einführung ihres Produkts in Unternehmen. Das gilt sowohl für die Definition der Teilprojekte als auch für die Projektorganisation und die verwendete Terminologie (siehe auch zum SAP Glossar [4]).

Die 6 Teilprojekte von uni.verse

Organisationsentwicklung

- Erarbeitung eines betriebswirtschaftlichen Modells
- Definition der Aufbau- und Ablauforganisation
- Unterstützung beim Change Management

SAP-Einführung

- Erstellung der Feinkonzepte auf Basis der Ergebnisse der Organisationsentwicklung
- Erstellung des Universitäts-Masters

Roll-Out und Schulung

- Durchführung aller Schulungen
- Adaptierungen des Universitäts-Masters an individuelle Anforderungen der Universitäten

Technik und Entwicklungen

- Bereitstellen der SAP-Systeme und Netzanbindungen
- Erstellen der Schnittstellen
- Datenübernahme aus Altsystemen

Betrieb und Services

- Betrieb der SAP-Systeme und Schnittstellen
- Betrieb des Desks im 2nd-Level-Support

Produktivsetzungsplanung

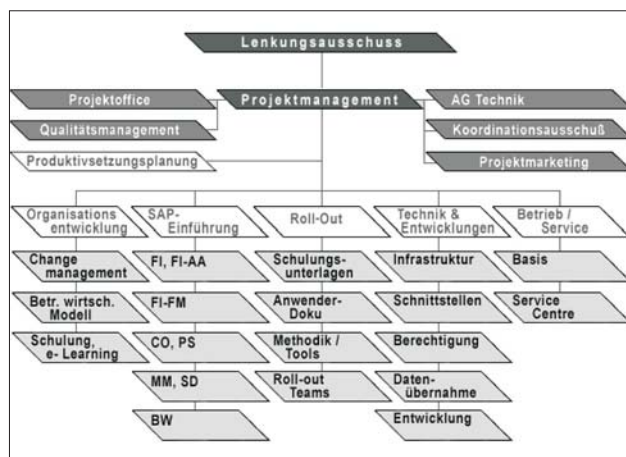


Abbildung 1: Projektorganisation uni.verse

Als „Aufsichtsrat“ des Projekts uni.verse agiert der Lenkungsausschuss. Er setzt sich aus von der Österreichischen Rektorenkonferenz nominierten Vertretern der Universitäten, des BMBWK, des BMF, des BRZ, des Instituts für Verwaltungsmanagement der Universität Innsbruck (als Koordinator vom BMBWK beauftragt) und von Siemens Business Services zusammen.

Der Koordinationsausschuss hat die Aufgabe, alle Universitäten einzubinden. Er wird regelmäßig über den Projektstand informiert, Inhalte werden diskutiert und bei Bedarf angepasst. Jede Universität hat einen Vertreter in den Ausschuss nominiert. Ihm kommt de facto keine Entscheidungsfunktion zu.

Die wesentlichen Entscheidungen werden vom Projektmanagement getroffen. Es ist für die Führung und Steuerung des Projektes verantwortlich und setzt sich aus jeweils einem Vertreter der Universität Wien, des Instituts für Verwaltungsmanagement, der Bundesrechenzentrum GmbH, der Firma SAP AG und der Firma Siemens Business Services GmbH zusammen. Der Lenkungsausschuss segnete meistens die Entscheidungen ab, die dann dem Koordinationsausschuss zur Kenntnis gebracht wurden.

An jeder Universität musste ein lokales Projektteam und ein lokaler Lenkungsausschuss eingesetzt werden. Zum Projektleiter an der TU Wien wurde Herr Mag. Christian Spranger (PCE) bestellt, zu seiner Stellvertreterin Frau Amtsdirektorin Eva Glatzer (Leiterin der Quästur). Ich bin Leiter des Teilprojekts „Technik & Entwicklung“.

Die Entwicklung eines einzigen „Masters“ für alle Universitäten, dessen Voreinstellungen dann im „Roll-out“ durch ein von SAP-Beratern durchgeführtes „Customizing“ an die Bedürfnisse der jeweiligen Universität angepasst werden sollte, hat sich in der Realität als nicht unproblematisch erwiesen. So hat sich bald herausgestellt, dass die strategische Vorgabe der Universitätsleitung der TU Wien, SAP so „dezentral als möglich“ einzuführen, um die bei uns so wichtigen Drittmittelaktivitäten in der Universität halten zu können, weiter vom „Master“ entfernt war als im Projekt vorgesehen. In zahlreichen TU-internen Workshops wurden die für uns wichtigen Geschäftsprozesse analysiert und dokumentiert. Selbst so komplizierte Abläufe wie die Umbuchungen bei Telefongebühren, Softwarelizenzen und Dienstleistungen des ZID konnten zufriedenstellend abgebildet werden. Andere gewünschte Prozesse führten zu „Change Requests“, das sind Änderungswünsche, für deren Realisierung die antragstellenden Universitäten aus Eigenmitteln aufkommen mussten.

Es ist der TU Wien dank des enormen Einsatzes unserer Projektleitung und des unschätzbaren Know-Hows von Herrn Dr. Alexander Redlein und seiner Gruppe – die in Zukunft als lokales SAP-Kompetenzzentrum der TU Wien („CCC“ = Customer Competence Center als Dienstleistung des neu geschaffenen Zentrums für Informations- und Facility-Management) tätig sein werden – und den wirklich guten Roll-out Beratern von IBM und SBS gelungen, mit vertretbaren Kosten die strategisch notwendigen „Change Requests“ zu realisieren. Einige unserer Forderungen wurden sogar nachträglich ins zentrale Master-Konzept übernommen und ihre Realisierung vom BMBWK finanziert, wie z. B. die ursprünglich nicht vorgesehene, scheinbar triviale Forderung, dass dezentrale Organisationseinheiten nicht berechtigt sein dürfen, die Konten anderer Organisationseinheiten einzusehen oder gar zu bebuchen.

Das CCC der TU Wien hat es auch übernommen, die TU-spezifischen Schulungsunterlagen zu erstellen (SBS war nur für den Master beauftragt), die Endanwenderschulungen durchzuführen, den so genannten „First-Level Support“ durchzuführen (an den Betreiber BRZ dürfen sich nur qualifizierte „Key-User“ unter Verwendung des SAP-Tools SLF / „Support Line Feedback“ wenden) und die Zugangssoftware an den Instituten zu installieren.

Den Universitäten wurden und werden vom BMBWF gemäß § 141 Abs. 4 UG 2002 unter dem Titel „Imple-

mentierungskosten“ die Kosten für die SAP-Lizenzen, die Entwicklungskosten von uni.verse sowie die Betriebskosten von uni.verse und uni.pers drei Jahre lang (2004 - 2006) neben dem Globalbetrag extra zugewiesen, ab dem Jahr 2007 sind dann die Betriebskosten im Rahmen der Leistungsvereinbarungen zu verhandeln und von den Universitäten aus dem laufenden Budget zu bezahlen.

Für den Betrieb der IT-Verfahren uni.verse und uni.pers sind von den einzelnen Universitäten Verträge mit dem BRZ abgeschlossen worden bzw. stehen unmittelbar vor dem Abschluss. Da das BRZ aufgrund gesetzlicher Bestimmungen weder Gewinne machen noch Verluste schreiben darf, müssen die Kosten für die Anschaffung und den Betrieb der Server-Hardware (Details siehe später) in den Betriebskosten mitkalkuliert werden. Das hat zu einer Mindestbindungsdauer von jeweils 5 Jahren (uni.verse 2004 - 2008, uni.pers 2005 - 2009) geführt. Wünscht eine Universität dennoch einen früheren Ausstieg aus dem Vertrag, so sind dem BRZ die dadurch nachweislich entstandenen Kosten – im Wesentlichen die verbleibenden Abschreibungsanteile der Hardwareinvestition – zu ersetzen.

Für mich sind die Universitäten ein wenig in die Situation von Kindern geraten, für die die wohlmeinenden und fürsorgenden Eltern eine verpflichtend mehrjährige Vereinsmitgliedschaft organisiert haben, den Mitgliedsbeitrag vom Taschengeld einbehalten aber gleichzeitig verlangen, dass die Kinder die Beitrittserklärung selbst unterschreiben, weil sie ja demnächst volljährig werden.

Einige Aspekte der SAP-Basistechnologie

Die SAP AG ist mit 29.000 Mitarbeitern und 7,4 Mrd. Euro Umsatz Europas größtes Softwarehaus und Weltmarktführer bei betrieblicher Software. Über 60.000 Installationen in mehr als hundert Ländern haben SAP R/3 dabei zu einem Quasi-Standard gemacht. Allerdings sind in dieser mächtigen Software bereits so viele Möglichkeiten „standardisiert“, dass bei der SAP-Einführung durch ein kompliziertes Customizing – meist unter Einbeziehung von speziell geschulten SAP-Beratern – die gewünschten, aber meist im Vorhinein vom Unternehmen noch nicht genau spezifizierten, Geschäftsprozesse modelliert werden müssen. Der voreingestellte Standard dient als „Reibebaum“ zur Begründung von Änderungen.

Die SAP-Basistechnologie beruht auf einer drei-schichtigen Client/Server-Architektur, wobei diesen Schichten innerhalb der Software jeweils spezifische Aufgaben zukommen. Im Einzelnen sind dies:

- die Präsentation der Anwenderoberfläche und Interaktion mit dem Benutzer (Präsentationsschicht, auch „SAP GUI“ genannt – SAP Graphical User Interface),
- die Ausführung und Abarbeitung der Anwendungslogik auf Basis einer gemeinsamen Infrastruktur (Applikationsschicht) sowie
- das Speichern, Lesen und Verwalten von Daten mithilfe einer Datenbank (Datenbankschicht, meist das Datenbanksystem eines Fremdherstellers wie Oracle oder Microsoft oder aber auch die inzwischen als Open-Source-Projekt veröffentlichte SAP-eigene Datenbank SAP DB).

Diese klare Trennung ermöglicht einerseits die Verteilung der Schichten auf verschiedene Rechner (vertikale Verteilung) und andererseits die Ausführbarkeit einer Schicht auf verschiedenen Rechnern bzw. Prozessoren gleichzeitig (horizontale Verteilung). Die Anwender benötigen lediglich die Präsentationsschicht auf ihrem Arbeitsplatzrechner, während die Applikations- und die Datenbankschicht auf separaten Servern installiert und ausgeführt werden können (siehe [5]).

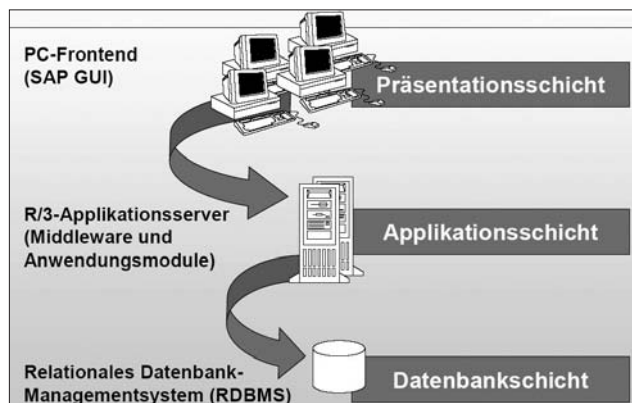


Abbildung 2: 3-Schicht Architektur von SAP R/3
(Quelle: IWI, www.iwi.uni-hannover.de)

Der normale R/3-Anwender, der die betriebswirtschaftlichen Funktionalitäten nutzt, benutzt als Arbeitsmittel ausschließlich die Präsentationsebene in der Form des SAP GUI. Zur Unterstützung unterschiedlichster Frontend-Hardware werden verschiedene SAP GUI-Realisierungen angeboten (siehe [6]).

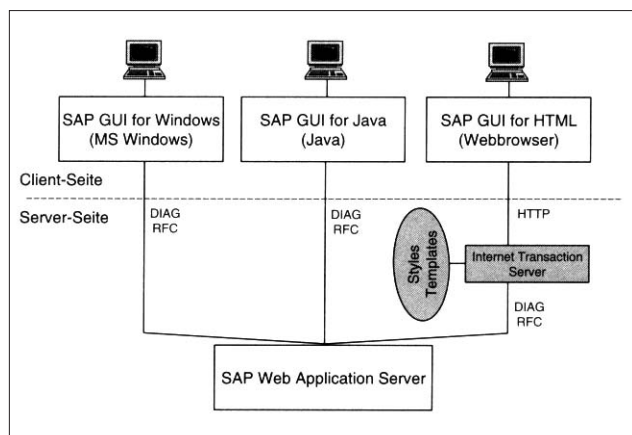


Abbildung 3: Front-End Varianten
(aus [6])

In der derzeit bei uni.verse eingesetzten Release 4.6c von SAP R/3 hat der SAP GUI für Windows den Vorteil, dass er als einziger den vollen Funktionsumfang der Präsentationsebene unterstützt. Nur im SAP GUI für Windows gibt es die Möglichkeit, für ABAP-Programme (ABAP steht für „Advanced Business Application Programming“ und ist eine von SAP geschaffene Programmiersprache für die Entwicklung von Anwendungsprogrammen im R/3-System), eine direkte Kommunikation mit beliebigen Werkzeugen wie Excel über das SAP-Schnittstellenprotokoll RFC (Remote Function Call) und das Microsoft-Schnittstellenprotokoll OLE/2 (Object

Linking and Embedding) aufzubauen. Dadurch kann R/3 z. B. über das SAP GUI auf die Daten eines Excel-Spreadsheets in beiden Richtungen zugreifen. Auch der Zugriff auf den Windows-Standarddrucker vom zentralen Drucker-Spooler des R/3-Systems erfolgt derzeit nur mit dem SAP GUI für Windows problemlos.

Der SAP GUI für HTML (Web-GUI) benötigt auf den Frontends nur einen Webbrowser, zur Umwandlung der Darstellung der Masken in HTML ist allerdings die Installation eines eigenen Internet Transaction Servers (ITS) erforderlich.

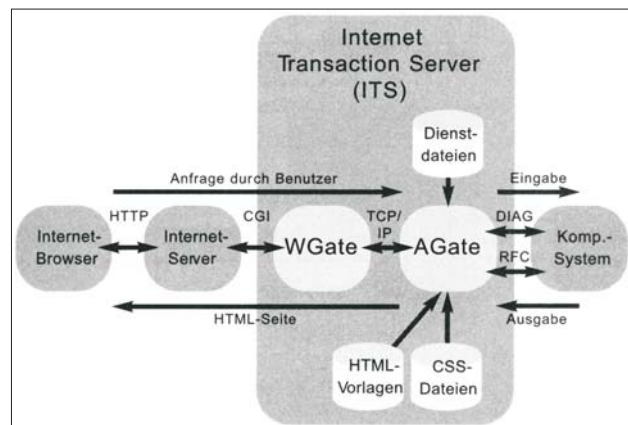


Abbildung 4: Protokollumsetzung durch einen ITS
(aus [5])

Der ITS konvertiert automatisch SAP-Bildschirme in HTML-Seiten, wobei er für ausgewählte Transaktionen vorgefertigte HTML-Darstellungen benutzt. Beim horizontalen Scrollen in breiten Masken muss allerdings jedesmal eine neue HTML-Seite erstellt werden, was zu merklichen Performance-Verlusten führt.

Erst mit der neuen Release 4.7 (SAP R/3 Enterprise) steht mit dem SAP Web Application Server eine neue Laufzeitumgebung zur Verfügung, die neben ABAP- auch Java-Programme in der Applikationsschicht ausführen kann. Da uni.verse bereits auf der Release 4.7 implementiert wird, steht im Jahr 2004 für uni.verse ein Release-Wechsel ins Haus. Das bedeutet zwar für die Universitäten einen zusätzlichen Aufwand, da die speziellen Customizing-Einstellungen und Change Requests erneut überprüft und abgenommen werden müssen, bietet aber auch eine Chance, die neue SAP-Technologie zu nutzen.

Die R/3-Softwarearchitektur erlaubt eine Verteilung der Applikationsebene auf mehrere so genannte „Instanzen“, die auch auf getrennten Rechnern betrieben werden können. Eine R/3-Instanz ist eine Gruppe von Prozessen mit dazugehörigen gemeinsam genutzten Speicherbereichen, die durch einen Dispatcherprozess gesteuert werden und auf dieselbe Datenbank zugreifen.

Ein „Mandant“ hingegen ist eine betriebswirtschaftlich selbständige Einheit. Sie umfasst auch eigenständige Bilanzen. Das Customizing wird vorwiegend mandantenabhängig vorgenommen. Es gibt allerdings Daten in der R/3-Datenbank, die systemweit gültig sind. Dazu gehören unter anderem ABAP-Programme, Funktionsbausteine und fast alle technischen Einstellungen. Diese Daten kön-

nen durch mandantenunabhängiges Customizing verändert werden und betreffen alle Mandanten innerhalb einer Instanz. „Somit eignen sich Mandanten innerhalb eines R/3-Systems z. B. für die Realisierung relativ unabhängiger Betriebsteile, weniger aber für die Umsetzung betriebswirtschaftlicher Abläufe vollständig unabhängiger Unternehmen“ (zitiert nach [5]).

In uni.verse wurden nur zwei Instanzen eingerichtet. Eine für die Wirtschaftsuniversität und eine für alle anderen 20 Universitäten. Genauer gesagt gilt das jeweils für das Entwicklungssystem, das Qualitätssicherungssystem und das Produktionssystem, die alle auf eigenen Instanzen und einer eigenen Hardware im BRZ laufen. Die Ausnahme für die WU resultiert aus der Tatsache, dass für die WU bereits seit einiger Zeit eine SAP-HR Lösung zur Personalverwaltung im Einsatz ist und die dafür notwendigen speziellen Einstellungen nicht auch für die anderen Universitäten übernommen werden konnten. Da sich die Universitäten eher früher als später zu eigenständigen und von einander unabhängigen Unternehmen entwickeln werden, die unterschiedliche Anforderungen an die Einführung neuerer SAP-Technologien und damit zusammenhängend an mandantenübergreifenden Einstellungen stellen werden, sind einerseits Konflikte zwischen den Universitäten und andererseits vermehrte Kosten für die an Innovation interessierten Universitäten absehbar und unvermeidlich.

Die Infrastruktur von uni.vers

Sowohl für die Implementierung von SAP R/3 als auch für den Produktivbetrieb musste eine entsprechende Serverhardware zur Verfügung gestellt werden. Die Hardware wurde vom BRZ bei HP beschafft und wird vom BRZ für die Universitäten betrieben. Grundlage war die Empfehlung von SAP, für R/3 ein dreistufiges System (Entwicklung, Qualitätssicherung und Produktion auf je einer eigenen Instanz) zu verwenden. Aufbauend auf diesen Vorgaben wurde von HP in Abstimmung mit dem BRZ ein Konzept vorgelegt, das der Lenkungsausschuss von uni.verse angenommen hat.

Der Vorschlag zur Realisierung der Serverhardware für den Produktivbetrieb ging dabei von folgenden Annahmen aus:

- eine „core“ SAP Instanz für 20 Universitäten
- eine eigene Instanz für die WU Wien
- eine Anbindung an das bestehende Storage Area Network (SAN) des BRZ

Für HP waren für die Dimensionierung der Serverhardware („Sizing“) die folgenden SAP-Benutzerklassen von Bedeutung, die sich aus dem geschätzten Zugriffsverhalten ableiten lassen.

- *High User*: aus technischer Sicht führt ein Benutzer dieser Klasse pro Woche durchschnittlich ca. 14.400 Dialogschritte aus. Dies entspricht 360 Dialogschritten pro Stunde (1 Dialogschritt alle 10 Sekunden). Ein Dialogschritt entspricht z. B. einem Bildwechsel.
- *Middle User*: aus technischer Sicht führt ein Benutzer dieser Klasse pro Woche durchschnittlich 4800 Dialogschritte aus. Dies entspricht 120 Dialogschritten pro Stunde (1 Dialogschritt alle 30 Sekunden).

- *Low User*: 1 Dialogschritt alle sechs Minuten im Durchschnitt.

Nach Abstimmung mit dem Projektmanagement wurde die hypothetische Systemlast der User folgendermaßen aufgeteilt:

High User:

10% der Professional User (Gleichzeitigkeit: 40%)

Middle User:

90% der Professional und 50% der Limited User bzw. Institutsuser (Gleichzeitigkeit: 40%)

Low User:

50% der Limited und 100% der Berichtuser (Gleichzeitigkeit: 20%)

Mit Professional, Limited, Instituts- und Berichtuser sind die vier Typen von SAP-Lizenzen gemeint, die für uni.verse vom BMBWK für und nach den Anforderungen der Universitäten angeschafft wurden. Es handelt sich dabei um personenbezogene Lizenzen, die den mit Username und Passwort geschützten Zugang zur SAP R/3-Applikation ermöglichen.

Für die Berichtuser wird, abgesehen von einem Puffer von 50 GB (für temporäres Abrufen von Berichten) kein Speicherplatz am Server bzw. SAN vorgesehen. Diese Vorgangsweise wurde damit begründet, dass Berichtuser keine Daten auf dem SAP-System speichern und lediglich ein bestimmter Swap-Space zur Verfügung stehen muss. Als weiterer Parameter für die Dimensionierung wurde berücksichtigt, dass die Session eines ITS-Benutzers automatisch geschlossen wird, nachdem dieser zehn Minuten am System inaktiv ist.

Die SAP-R/3 Produktivinstanz wird an zwei getrennten Standorten auf HP Superdome Systemen als MC/ServiceGuard Cluster abgebildet und wird hochverfügbar im Bundesrechenzentrum bzw. im Parallelrechenzentrum betrieben. Die Instanz für BW (SAP Applikation Businesswarehouse) wird ebenfalls hochverfügbar in einer HP-UX-Partition auf diesen Systemen betrieben.

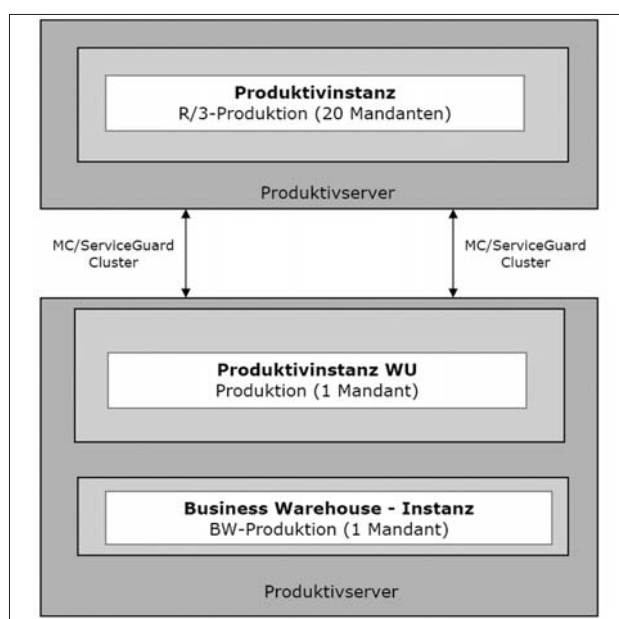


Abbildung 5: Serverhardware für das Produktionssystem im BRZ

Ein MC/ServiceGuard Cluster ist ein hochverfügbares System von HP 9000 Serie 800 Servern („Nodes“), das genügend Redundanz an Hardware- und Softwarekomponenten besitzt, damit kein „single point of failure“ zu einer Unterbrechung des Services führt. Anwendungsprozesse werden in „Packages“ zusammengefasst. Im Falle eines einzelnen Fehlers eines Services, einer Betriebssystemkomponente, einer CPU, eines Speicherblocks, eines Nodes, eines Netzwerks oder einer anderen überwachten Ressource, kann der MC/ServiceGuard automatisch die Kontrolle des Packages auf einen anderen Node im Cluster transferieren, sodass die Services nach einer minimalen Unterbrechungszeit verfügbar bleiben.

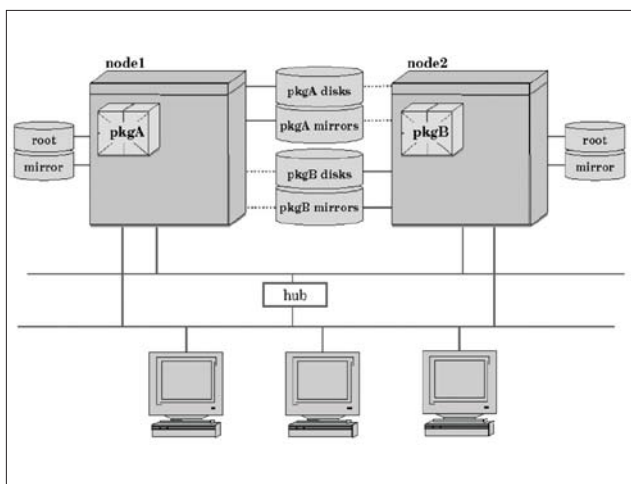


Abbildung 6: MC/ServiceGuard Cluster Konfiguration

Abb. 6 zeigt die Situation eines typischen MC/ServiceGuard Clusters. Das Package A läuft auf Node 1, Package B auf Node 2. Jedes Package hat eine eigene Gruppe von zugeordneten Platten, die auch noch gespiegelt sind (Raid). Obwohl beide Nodes physisch an beide Raids angeschlossen sind, hat immer nur einer der beiden Nodes den exklusiven Zugriff (durchgezogene Linie). Das Netzwerk ist ebenfalls redundant ausgelegt. MC/ServiceGuard verwendet TCP/IP auch für die Übertragung und Überwachung von „heartbeat messages“, die einen normal funktionierenden Node signalisieren.

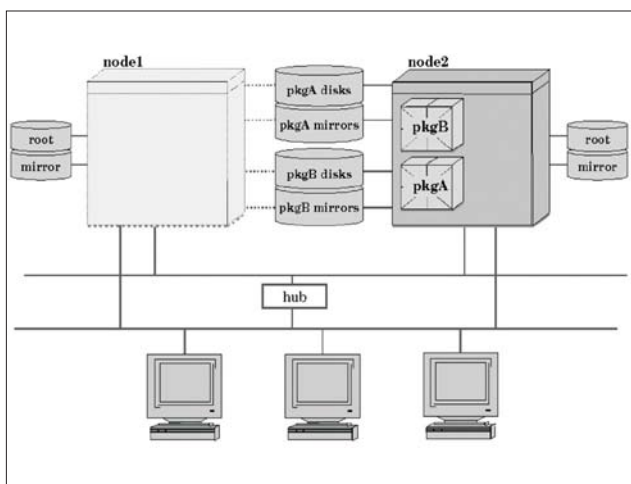


Abbildung 7: MC/ServiceGuard Cluster nach Failover

Im Fehlerfall überträgt MC/ServiceGuard die Kontrolle des Packages A auf den nächsten verfügbaren Node. Abb. 7 zeigt die Situation nach der erfolgreichen Fehlerübergabe. Auf Node 2 laufen jetzt beide Packages (natürlich mit einer reduzierten Performance) und Node 2 hat exklusiven Zugang zu beiden Raids.

Weil der MC/ServiceGuard Cluster im BRZ die Superdome Nodes an zwei Standorten mit einer redundanten Anbindung an das SAN und LAN einsetzt, wird wirklich eine höchstmögliche Verfügbarkeit der Applikationen von uni.verse gewährleistet.

Die beiden Systeme werden in je zwei Hardware-Partitionen unterteilt:

Server 1:	
Npar0: SAP BW	6 CPUs PA8700 875 MHz, 12 GB RAM
Npar1: SAP R/3	6 CPUs PA8700 875 MHz, 18 GB RAM
Server 2:	
Npar0: SAP BW	6 CPUs PA8700 875 MHz, 12 GB RAM
Npar1: SAP R/3	6 CPUs PA8700 875 MHz, 18 GB RAM

Das Entwicklungssystem wird auf einem HP rp5470 Server und das Qualitätssicherungssystem auf einem HP rp7410 Server laufen. Beide Server verfügen über jeweils 6 CPUs PA8700 750 MHz und 9 GB RAM .

Zugang über AConet und „Portal Austria“

Der Wunsch der Universitäten, über das AConet auf die bereitgestellten Applikationsserver im BRZ mittels SAP GUI bzw. Web-GUI/ITS zugreifen zu können, wurde berücksichtigt. Das BRZ hat einen Zugang zu AConet im Rahmen des „ACO-IX“ erhalten, der genügend Bandbreite für den Applikationszugriff zur Verfügung stellt. Nach den internen Richtlinien des BRZ muss für den Zugriff vom Internet auf Applikationen, die vom BRZ bereitgestellt werden, das „Portal Austria“ als Schnittstelle fungieren. Die Applikation uni.verse wurde daher ins „Portal Austria“ integriert.

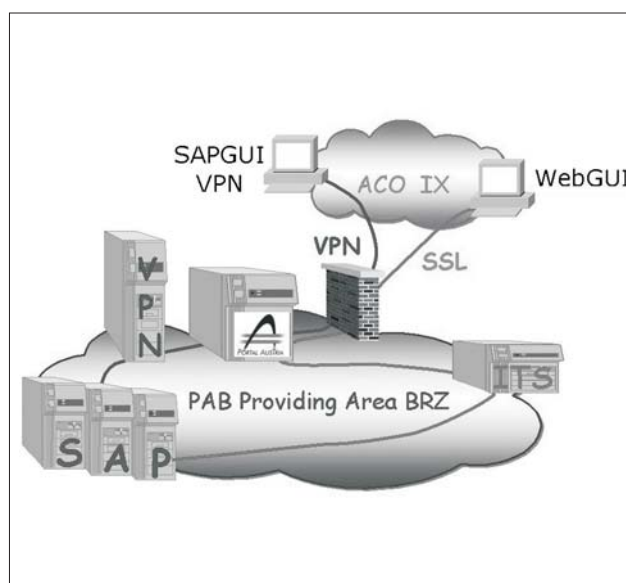


Abbildung 8: Schematische Darstellung der Systemlandschaft im BRZ

Im Rahmen des „Portal Austria“ soll es berechtigten Benutzern ermöglicht werden, einfach und einheitlich auf Funktionalitäten von SAP R/3 zugreifen zu können, ohne sich explizit bei einer bestimmten Applikation anmelden zu müssen. In diesem „Single Sign On“-Verfahren werden dem Benutzer automatisch alle ihm zugeordneten SAP-Module zur Verfügung gestellt und er kann aus dem Browser den SAP GUI für Windows oder den SAP-Web-Client (SAP GUI für HTML) starten. Da das System SAP R/3 derzeit über keine befriedigende Lösung zur erforderlichen Datenverschlüsselung bei der Kommunikation mit dem SAP GUI für Windows verfügt, wird eine sichere Datenübertragung über ein VPN (Virtuelles Privates Netzwerk) gewährleistet. Der VPN-Konzentrator im BRZ kann bis zu 5000 Client-Sitzungen simultan betreiben. Der sichere Zugang zum ITS erfolgt über Secure Socket Layer (SSL).

Das „Portal Austria“ wird auch als Werkzeug für die Verwaltung der einzelnen Benutzer eingesetzt. Über die verteilte Administration ist es den Administratoren der Universitäten vorbehalten, entsprechende Berechtigungen zu vergeben und diese auch in ihrem Bereich unbürokratisch zu verwalten. Für die TU Wien wird diese Tätigkeit vom CCC durchgeführt.

Anforderungen an die Hard- und Software auf Seiten der Institute (Clients)

Im Folgenden werden kurz die Empfehlungen und Vorgaben seitens der Projektleitung zur Abdeckung der Leistungsanforderungen für Applikationen rund um uni.verse vorgestellt. Die technischen Voraussetzungen beziehen sich dabei nicht nur auf den Einsatz der SAP GUIs, sondern auch auf die Verwendung von Applikationen wie Internet-Browser und Microsoft Office. Bei Neubeschaffung von Rechnern sollte darauf geachtet werden, dass damit zumindest zwei Jahre ohne Einschränkung, und danach ein Jahr ohne unzumutbare Verzögerungen und Wartezeiten, gearbeitet werden kann.

Der ZID bietet im Rahmen der „Systempflege für Arbeitsplatzrechner“ (sts.tuwien.ac.at/pss/) an, die Tauglichkeit eines Institutsarbeitsplatzes als SAP R/3-Client zu überprüfen bzw. herzustellen. Die notwendige Zugangssoftware (SAP GUI und VPN Client) steht im Rahmen der Campus Software zum kostenlosen Download bereit. Die Installation der Zugangssoftware wird in der Regel vom CCC der TU Wien durchgeführt.

Anforderungen an die Hardware (Empfehlungen)

CPU:

Intel Pentium III ab 1000 MHz (FC-PGA)
Intel Pentium 4 ab 1,5 GHz (Socket-478)
AMD Athlon XP ab 1200 MHz (Socket-A)

Hauptspeicher:

256 MB DIMM / 133 MHz
256 MB DDR-DIMM / PC 2100
256 MB RIMM / 800 MHz

Festplatte:

40 GB E-IDE (UDMA-100)
36 GB SCSI-LVD

CDROM:

40fach CDROM (ATAPI, SCSI)
10fach DVD-ROM (ATAPI, SCSI)

Grafikkarte:

AGP-Grafikkarte (16MB)

Netzwerk:

10/100 Mbit PCI Netzwerkkarte Ethernet

Monitor:

17 Zoll CRT / 96 kHz
19 Zoll CRT / 110 kHz
15 Zoll LCD / TFT Analog
17 Zoll LCD / TFT DVI

Tastatur:

104 Tasten Windows-kompatibel (mit Euro-Symbol)
105 Tasten IBM-kompatibel (mit Euro-Symbol)

Maus:

n Tasten PS/2 oder seriell mit Scrollrad
n Tasten PS/2 oder seriell mit Scrollrad und optischer Abtastung

Audiokarte:

„Soundblaster Live!“-kompatible PCI-Karte
Audiokarte „OnBoard“

Lautsprecher:

Computer-Lautsprecher Leistung min. 10 Watt
Mikrofon mit PC-Anschluss
(ohne Phantom-Speisung)
Aktive Kopfhörer (Impedanz kleiner als 200 Ohm)

Anmerkung: Im Projekt uni.verse könnten diverse Schulungen im Multimedia-Format vorgetragen werden. Um multimediale Schulungsinhalte verstehen zu können, wird ein Schallwandler benötigt. Wenn es sich um eine Lern-Station handelt oder der Benutzer ein Einzelbüro hat, so können ohne weiteres aktive Lautsprecher verwendet werden. In Großraumbüros ist die Verwendung von Kopfhörern anzuraten, um weitere Kollegen nicht bei der Arbeit zu stören.

Anforderungen an die Software (Vorgaben)

Betriebssystem:

Windows NT 4.0 SP6a:
(Es wird darauf hingewiesen, dass Windows NT von Microsoft nicht mehr in der Wartung steht.)

Windows 2000 SP2

Windows XP

Windows 98SE (nicht secure !)

Anmerkungen:

Für Betriebssysteme auf Apple Computer steht kein eigener SAP-GUI zur Verfügung. Der SAP GUI für HTML kann mit Einschränkungen verwendet werden, der SAP GUI für Java kommt erst Mitte 2004 (Release 4.7).

Windows 2003 Server funktioniert derzeit nicht.

Viewer Tools:

Als Viewer Tool ist Adobe Acrobat Reader ab der Version 4.05 erforderlich.

Web-Browser:

Für die Anzeige der On-line-Hilfe ist alleinig der MS Internet Explorer ab der Version 6.0 SP1 zulässig, da Netscape Navigator aufgrund einer anderen internen Objektstruktur nicht kompatibel ist.

Office-Integration:

SAP R/3 bietet ein COM-Gateway zu Microsoft Excel. Für das Anzeigen von Berichten ist somit der Einsatz von Excel ab der Version 97 erforderlich. Es sei darauf hingewiesen, dass vom gesamten Office-Paket nur Excel benötigt wird, welches auch unterstützt wird.

Anforderungen an die Zugangssoftware (Vorgaben)

SAP-GUI für Windows:

SAP-GUI 6.20 (GUI-Patchlevel 36, BW-Patchlevel 9)

VPN-Client:

Cisco VPN-Client 4.0.1

Portal Austria-Integration:

Java Runtime Environment 1.4.2_01

Files für die Portal Austria-Integration (SSO-Client)

Anmerkung: Die Softwarepakete sind am Softwaredistributionsserver des ZID hinterlegt.

Schlussbemerkung

Dieser Artikel ist zwar ziemlich lang geworden und doch konnte ich nicht über alles schreiben, was ich gerne losgeworden wäre. So ist zum Beispiel die Frage der Schnittstellen zu anderen Systemen spannend wie ein Krimi. Im Projekt uni.verse wurden bisher vom Lenkungsausschuss nur die Schnittstellen zum Bibliothekssystem ALEPH und zur Bundesbesoldung in Auftrag gegeben. Was wird mit den anderen Schnittstellen geschehen, die für „ein möglichst reibungsloses Zusammenspiel mit den IT-Anwendungen der Universitäten“ (Projektauftrag) so wichtig sind? Was wird das die TU Wien kosten? Welche Schnittstellentechnologien werden möglich, welche davon wirklich eingesetzt werden? Fünf Jahre sind eine lange Zeitspanne, in der sich auch die Technologiekonzepte der SAP AG und des BRZ mehrfach ändern werden. Können wir uns zurücklehnen und einfach freuen, wenn die Bilanz richtig herauskommt?

Den Universitäten wurden im Projekt eine ganze Reihe von Pflichten und Verantwortlichkeiten auferlegt. Erwähnt habe ich schon die Administratoren der User am „Portal Austria“, die Verantwortung für die Endanwenderschulung, die „Key-User“ und den „First-Level Support“. Nicht erwähnt habe ich die aufwendige Einrichtung und Pflege der Rollen und Berechtigungen im R/3-System, die bei einer dezentralen Nutzung wie an der TU Wien einen wirklich großen Aufwand darstellt. Nicht erwähnt habe ich den hohen Aufwand für die Pflege der Stammdaten, zu denen auch Kostenstellen, Finanzstellen, Innenaufträge und vieles mehr gehören. Nicht erwähnt habe ich die Schnittstellenverantwortlichen, die die Transaktionslogs

kontrollieren und im Fehlerfalle die richtigen Aktionen setzen müssen. Was machen Universitäten, die nicht bereits mit einem so großen SAP Know-How starten konnten wie wir? Steht überall der Aufbau von lokalen CCCs auf der Tagesordnung? Werden wir uns in Zukunft nur mehr mit SAP beschäftigen?

Ich glaube nicht. Erstens werden wir es nach einer gewissen Anlaufphase sicher schaffen, mit den neuen rechtlichen Randbedingungen und der betriebswirtschaftlichen Software zurechtzukommen. Und zweitens wird es andere neue und spannende Projekte geben.

Literatur

- [1] Projekt Homepage „uni.verse“
www.uni.verse.at
- [2] Universität Innsbruck, Projekt SAP
www2.uibk.ac.at/fakten/leitung/ректор/sap/
- [3] Newsletter zur SAP-Einführung an der TU München: www.sap.tum.de/sapalott.html
- [4] SAP Glossar:
help.sap.com/saphelp_46c/helpdata/de/35/2cd77bd7705394e10000009b387c12/frameset.htm
- [5] SAP R/3 Systemadministration
Sigrid Hagemann, Liane Will, SAP Press, 2003
- [6] mySAP Technology
Günther Färber, Julia Kirchner, Galileo Press, 2003

Open Source im öffentlichen Bereich

Udo Linauer

Stabsstelle IKT-Strategie des Bundes

udo.linauer@cio.gv.at

Gerne habe ich die Einladung angenommen, über die Aktivitäten im Bereich freier Software (Open Source) im öffentlichen Bereich zu berichten. Nicht ganz zu Unrecht besteht der Eindruck, dass in Österreich diesbezüglich nicht viel los sei, im Vergleich zu Deutschland in etwa. Dass dies nur zum Teil stimmt, möchte ich belegen, wohin der Zug abfährt und wo noch Probleme vorliegen, wird den zweiten Teil dieses Berichts bestimmen. Die gute Nachricht aber vorweg: Allgemein herrscht Einigkeit, dass das Modell „Open Source“ auch auf lange Sicht Vorteile bringen wird und es sich dabei keinesfalls um eine irrelevante Modeerscheinung handelt.

Vorarbeiten

Open Source ist (noch) keine Feder, mit der sich Entscheidungsträger im öffentlichen Bereich gerne schmücken. Was auch immer der Grund dafür sein mag, hinter den Kulissen tut sich jedoch einiges. In der Öffentlichkeit wird zumeist die Wichtigkeit offener Standards und Schnittstellen betont, nicht zuletzt auch von der für Entwicklung und Umsetzung von E-Government verantwortlichen Stabsstelle IKT-Strategie im Bundeskanzleramt, für die ich arbeite. Nur so könne in einer heterogenen IT-Landschaft Vernetzung funktionieren, E-Government stattfinden. Das vordringliche Interesse auf technischer Ebene liegt also in den Open Interfaces, die Stabsstelle hat jedoch nie verschwiegen, dass deren Umsetzung ausgezeichnet mit Open Source zu erreichen sei. Auf einer anderen Front arbeitet das Bundesministerium für Wirtschaft und Arbeit (BMWA), das eine Studie mit dem Titel „Auswirkungen von Open-Source Software auf den Arbeitsmarkt“ in Auftrag gab, um den Einfluss des Einsatzes von Open Source Produkten auf den lokalen Arbeitsmarkt zu erforschen. Die Ergebnisse finden Sie unter: www.open-source.at.

Dies heißt aber nicht, dass nicht an konkreten Projekten gearbeitet wird und der Boden für weiteren Einsatz von Open Source Produkten bereitet werden soll. Worin

bestehen denn nun diese Aktivitäten? Zuallererst sollte eine Änderung in der Vorgehensweise hervor gestrichen werden. Bei großen Projekten wird inzwischen darauf Wert gelegt, dass Schnittstellen in technologieunabhängiger Form spezifiziert werden und somit selbst Open Source sind. Beispiele dafür sind die Bürgerkarte, die ja bekannterweise nicht eine physikalische Karte ist, sondern vielmehr ein Konzept, in dem Kernfunktionen wie Erstellung von elektronischen Signaturen und zertifikatsbasierte Authentifizierung beschrieben wird. Das gleiche gilt für den verwaltungsinternen Verzeichnisdienst (www.cio.gv.at/it-infrastructure/directory-services/), bei dem es leichter gewesen wäre, das eine oder andere kommerzielle Produkt zu wählen oder auch für den Portalverbund (www.cio.gv.at/it-infrastructure/portal/), der es Betreibern von Portalen erlaubt, die Authentifizierung und Autorisierung an andere Portale zu delegieren.

Die Anstrengungen, Anforderungen an Software technologieunabhängig zu beschreiben, verfolgen ein Modell modularer Softwarekomponenten. Die gegenseitigen Abhängigkeiten und die daraus resultierende Bevorzugung von gewissen Produktfamilien soll abgestellt werden. Damit erhöhen sich auch die Chancen von neuen Produkten, unter anderem auch von Open Source Software.

In dieselbe Kerbe schlägt ein offizieller Beschluss des IKT-Boards, der besagt, dass neu anzuschaffende Server-

Hardware linuxtauglich sein muss (www.cio.gv.at/ikt-board/beratungen/open-source/recommendation/). Einen Schritt weiter noch geht der Beschluss (www.cio.gv.at/ikt-board/beratungen/security/discussion/) desselben Gremiums zum Thema ausfallsichere Applikationen mit der Feststellung: „... Für neue Anwendungen wird in den höheren Schutzklassen, die ein Ausweichsystem erfordern, in Hinkunft Linux als Systembasis einzusetzen sein.“ Das heißt, dass in dem besonderen Umfeld der ausfallsicheren Applikationen aus Kosten- und Effizienzgründen Linux der Vorzug gegeben wird.

Abschließend sind die Bestrebungen der Bundesbeschaffungsgesellschaft zu erwähnen, die Geschäftspartner für einen Rahmenvertrag im Bereich der Anschaffungen und Dienstleistungen im Bereich Open Source sucht.

„Governmental“ Open Source

Immer mehr Eigenentwicklungen laufen im öffentlichen Bereich unter der Bezeichnung „Governmental Open Source“. Damit wird Software bezeichnet, die Körperschaften des öffentlichen Rechts im Quellcode und meistens auch kostenlos zur Verfügung steht. Die Intention dafür ist dieselbe wie bei „echter“ Open Source, nämlich der Wunsch nach gemeinsamer Weiterentwicklung und Verbesserung, sowie der einfachen Adaption an spezielle Anforderungen. Warum werden diese Programme nicht gänzlich freigegeben? Oft sind Bereiche des E-Government und der elektronischen Signatur betroffen, in denen es wenige Anbieter gibt, denen nicht aus Steuermitteln finanzierte Konkurrenz gemacht werden soll. Beispiele für derartige Software sind die so genannten Basismodule für Signaturerstellung und Prüfung, sowie für Personenidentifizierung mittels Bürgerkarte (www.cio.gv.at/onlineservices/basicmodules/).

„Echte“ Open Source

Wir erreichen langsam aber sicher den Aspekt, der in der Regel unter dem Titel Open Source Schlagzeilen macht, aus unserer Sicht aber nur einen Teil des Gesamt-szenarios darstellt, nämlich den Einsatz von Open Source Produkten und deren (Mit)Entwicklung. Die Durchdringung mit Open Source Produkten ist in den einzelnen Körperschaften ganz unterschiedlich weit gediehen. Man-

che Organisationseinheiten haben dahingehend eine Vorreiterrolle, andere beginnen erst mit dem Einsatz. Wir wollen uns auf eine Vorreiterin konzentrieren. Die im Vergleich mit München viel gescholtene Stadt Wien hat seit Jahren ausschließlich UNIX-Fileserver im Einsatz, von denen inzwischen 75% Linuxserver sind. Ähnlich verhält es sich bei den Webservern. Dementsprechend gibt es in solchen Organisationen auch Personen, die Administration und Wartung von einer großen Anzahl von Servern beherrschen, Software adaptieren und auch selbst programmieren. Dabei entstand ein Umfeld, in dem es möglich ist, Lösungen selbst zu programmieren, wenn kein geeignetes Produkt erhältlich ist. So wurde in Wien unlängst die auf ZOPE (www.zope.org) basierende Groupware „vieW4“ (= „vienna World Wide Web Workgroups“) entwickelt (www.cio.gv.at/service/newsletter/Newsletter_05_03.html). Ich kann nur empfehlen, einen Blick auf dieses Projekt zu werfen. Diese Groupware wird inzwischen schon in einigen anderen Behörden eingesetzt und ist ein gutes Beispiel für Open Source Entwicklungen im öffentlichen Bereich.

Problembereiche

Leider gibt es noch immer Bereiche, in denen keine Open Source Produkte existieren bzw. deren Einsatz nicht möglich ist. Ein heikles Thema ist jenes der sicheren elektronischen Signatur, die derzeit nur mit Signaturkarten realisiert ist. Es gibt keine Lösungen diesseits von Microsoft Windows. Um dieses Problem zu entschärfen, führt das neue E-Government Gesetz (labs.cio.gv.at/egovg/) die so genannte Amtssignatur ein. Es handelt sich dabei um eine zeitlich befristete Signaturvariante, die weniger rigiden Sicherheitsvorschriften unterliegt und z. B. unter dem plattformunabhängigen Einsatz von Mobiltelefonen realisiert werden könnte.

Weiters gibt es Probleme mit in Fachapplikationen üblichen Fat-Clients, die bisweilen die freie Wahl von Betriebssystemen und / oder anderer Software unmöglich machen.

Zuletzt möchte ich auch noch darauf hinweisen, dass die Ausbildung starke Schlagseite hat. Leider wird der Schulung mit dem Umgang mit Open Source Produkten noch immer viel zu wenig Aufmerksamkeit geschenkt.

Itanium 2 und numerisch intensives Rechnen

Ernst Haunschmid

Egal ob Quantentheorie, Biochemie oder Mikroelektronik, der Bedarf an leistungsfähigen Rechnersystemen ist ungebrochen. Neue Prozessoren wie der Itanium 2 kommen da gerade richtig. Bei all der Rechenleistung stellt sich aber auch die Frage einer objektiven Bewertung derselben.

SPEC Benchmarks

Die Standard Performance Evaluation Corporation (SPEC) ist eine Non-Profit Organisation mit der Zielsetzung, aussagekräftige Benchmarks für aktuelle Hochleistungsrechner zu erstellen und zu etablieren. Die von den Mitgliedern und Lizenznehmern eingereichten Ergebnisse der Benchmarks werden von der SPEC überprüft und veröffentlicht (www.spec.org).

Zur Bewertung von Rechnersystemen für numerisch intensives Rechnen wird gerne der SPEC CPU2000 herangezogen. Dies ist eine Sammlung von *real world* Applikationen, die die Leistungsfähigkeit von CPU, Hauptspeicher und Compiler des untersuchten Rechnersystems testen soll.

Der SPEC CPU2000 besteht aus zwei Teilen; SPEC int2000 besteht aus 12 C/C++ Programmen, bei denen die Integer Leistung dominiert, während bei SPECfp2000 die Gleitpunktleistung im Vordergrund steht. Da bei technisch-naturwissenschaftlichen Anwendungen (Modellbildung, Simulation) meistens die Gleitpunktleistung ausschlaggebend ist, wird im Folgenden näher auf den SPECfp2000 eingegangen; die Programme des SPEC fp2000 sind in Tabelle 1 angeführt.

Jedes dieser Programme wird auf dem zu testenden System kompiliert und die Laufzeit ermittelt; diese wird in Relation zu einer Referenzlaufzeit gesetzt und aus dem geometrischen Mittel dieser Faktoren wird der SPEC fp2000 Wert berechnet. Als Referenzsystem dient eine Sun Ultra 5/10 (300 MHz), die den Wert 100 erhält. (Ein SPECfp2000 Wert von 1500 bedeutet daher, dass das betreffende System 15 mal schneller arbeitet als das Referenzsystem.)

Dabei gibt es 2 Varianten: bei der Ermittlung des *base* Wertes müssen Einschränkungen bei der Art und der

Anzahl der Compiler-Optionen berücksichtigt werden, während beim *peak* Wert diese Einschränkungen wegfallen. In diesem Artikel sind immer die *peak* Werte angeführt.

Benchmark	Sprache	Anwendungsgebiet
168.wupwise	Fortran 77	Physik/Quantenchromodynamik
171.swim	Fortran 77	Meteorologie/Wasserströmungen
172.mgrid	Fortran 77	Multi-grid Gleichungslöser
173.applu	Fortran 77	Partielle Differentialgleichungen
177.mesa	C	3D Graphik Bibliothek
178.galgel	Fortran 90	Strömungsdynamik
179.art	C	Bilderkennung mit neuronalen Netzwerken
183.equake	C	Ausbreitung von seismischen Wellen
187.facerec	Fortran 90	Bildbearbeitung
188.amp	C	Atombewegungen in einem Protein-Molekül
187.facerec	Fortran 90	Bildbearbeitung
188.amp	C	Atombewegungen in einem Protein-Molekül
189.lucas	Fortran 90	Zahlentheorie/Primzahltest
191.fma3d	Fortran 90	Crash Simulation mit finiten Elementen
200.sixtrack	Fortran 77	Partikel in einem Teilchenbeschleuniger
301.apsi	Fortran 77	Meteorologie/Schadstoffausbreitung

Tabelle 1: Die Programme des SPECfp2000

Itanium

Der Itanium Prozessor war die erste Generation einer neuen Prozessorarchitektur, die von Hewlett-Packard und Intel gemeinsam entwickelt wurde und von Intel produziert und vermarktet wird.

Computer System	Prozessor	OS	SPECint2000	SPECfp2000
HP rx2600	Itanium 2 1.5 GHz, 6 MB	Redhat AS 2.1	1322	2119
IBM p655	Power4+ 1.7 GHz	AIX 5.2	1103	1678
Intel D875PBZ	Pentium 4 EE 3.2 GHz	Windows XP	1620	1494
AMD	Athlon FX-51 2.2 GHz	Windows XP	1447	1423
HP ES45 68	Alpha 21264C 1.25 GHz	Tru64	928	1365
Intel D875PBZ	Pentium 4 3.2 GHz	Windows XP	1330	1285
AMD A4800	Opteron 144 1.8 GHz	Windows 2003	1170	1219
Sun Blade 2000	Ultra SPARC III 1.2 GHz	Solaris 9	722	1118
SGI Origin3200	Mips R14000 600 MHz	IRIX 6.5	500	529
HP rp5470	PA-8700 750 MHz	HPUX 11i	549	522

Tabelle 2: SPEC CPU2000 Werte einiger Rechnersysteme

Die Anfänge der Itanium-Architektur reichen bis ins Jahr 1980, als HP Labs eine Architektur zu entwickeln begann, die die damals von HP angebotenen Computersysteme einander ähnlicher machen sollte. Daraus entstand die so genannte PA-RISC-Architektur, die auf der Mehrzahl der Unix Systeme von HP noch immer im Einsatz ist.

Weil man sich bewusst war, dass die RISC-Architektur irgendwann an ihre Grenzen stoßen würde, initiierte HP Labs Anfang 1989 ein Forschungsprogramm zum Thema Instruction Level Parallelism (ILP) mit dem Ziel, die Architektur des Very Long Instruction Word (VLIW) auf allgemeinere Zwecke und Belange umzulegen. Aus diesem Forschungsprogramm, das bis 1996 lief, gingen die EPIC-Architektur und die entsprechende Compiler-Technologie hervor.

Etwa zur gleichen Zeit, als die Arbeit an ILP begann, startete HP Labs ein eigenes Programm für den Aufbau einer EPIC-Architektur, die PA-RISC ersetzen sollte. 1993 hatte man die PA-WideWord-Architektur entwickelt – die Basis der Zusammenarbeit zwischen HP und Intel und Grundstein der Itanium Prozessor Spezifikation (ursprünglich IA-64 genannt).

Itanium wurde als parallele Hochleistungsarchitektur entwickelt, die mehr Befehle in einem Takt ausführt als die Vorgängerarchitekturen. Das ist möglich, weil die Last des Befehls-Schedulings auf den Compiler abgewälzt wird; der Compiler kann zur Compile-Zeit die einzelnen Instruktionen für maximale Parallelität ordnen; zur Laufzeit ist kein Befehls-Scheduling mehr notwendig (und auch nicht möglich).

Die Effizienz Itanium-basierter Systeme hängt ganz wesentlich von der Verfügbarkeit entsprechender Compiler ab. Die erste Generation des Itanium Prozessors konnte unter anderem aus diesem Grund nicht überzeugen.

Die neueste Generation des Itanium 2 Prozessors soll, glaubt man den Aussagen der diversen Anbieter, alles besser und vor allem schneller können.

SPECfp2000

Die erste Version des Itanium Prozessors konnte mit seiner eher mäßigen Leistung nicht überzeugen. Eine der

Ursachen neben dem fehlenden Compiler-Support war die Konzeption des Speichersubsystems, das dazu führte, dass der Prozessor vornehmlich auf den Hauptspeicher warten musste. Mit riesigen on-chip L3 Caches mit bis zu 6 MB versucht Intel beim aktuellen Itanium 2 dieses Manko auszugleichen. Die SPEC CPU2000 Werte belegen den Erfolg dieser Strategie eindrucksvoll. Wie weit diese Leistung auch in anderen Applikationen erreichbar ist, bleibt aber offen. Die Tabelle 2 gibt einen Überblick über die SPEC CPU2000 Werte einiger Computer Systeme.

Die extrem hohen SPEC CPU2000 Werte des Itanium 2 Prozessors beruhen zumindest zu einem Teil auf seinem 6 MB großen Level 3 Cache; einige Programme des SPEC CPU2000 (beispielsweise 179.art) finden im L3 Cache Platz, zeitraubende Zugriffe auf den Hauptspeicher können dadurch minimiert werden. Damit wird aber auch eine Zielsetzung des SPEC CPU2000 unterlaufen: die Leistungsfähigkeit des Hauptspeichers geht in die SPEC CPU2000 Werte kaum mehr ein. Da diese Problematik nicht nur für den Itanium 2 gilt, wird von SPEC bereits seit 2 Jahren an einem Nachfolger gearbeitet, dem SPEC CPU2004.

Tabelle 3 gibt die relativen SPECfp2000 Werte einiger Itanium 2 Konfigurationen wieder.

Bemerkenswert sind die Unterschiede in den Resultaten zwischen Linux/Intel und HPUX bei identer Hardware. Die beiden Compiler haben offenbar jeweils ihre Schwächen; ein Teil der Leistungsfähigkeit des Itanium 2 wird derzeit nicht ausgenutzt.

Der SPEC CPU2000 ist ein allgemein anerkannter Benchmark und die Hersteller zitieren gerne (die für sie günstigen) Resultate. Sie sollten aber nicht überbewertet werden; es gibt genügend Applikationen, deren Laufzeitverhalten auf den einzelnen Systemen nicht mit den SPEC CPU2000 Werten korrelieren. Eine Kaufentscheidung nur aufgrund eines beeindruckenden Benchmark-Wertes zu treffen, könnte mit unliebsamen Überraschungen enden.

In der Tabelle 4 sind die SPECfp2000 Werte detailliert dargestellt; der Wert des jeweils besten Systems ist hervorgehoben. Obwohl die HP rx2600 mit dem Itanium 2 Prozessor mit Abstand den besten SPECfp2000 Wert vorweisen kann, wird sie bei der Hälfte der Benchmark-Programme von anderen Systemen (zum Teil deut-

Prozessor	Itanium 2	Itanium 2	Itanium 2	Itanium 2	Itanium 2
MHz	900	900	1000	1000	1500
L3 Cache in MB	1.5	1.5	3.0	3.0	6.0
OS	Redhat	Redhat	Redhat	HPUX	Redhat
Compiler	Intel 7.0	Intel 7.1	Intel 7.0	HP	Intel 7.1
168.wupwise	1.00	1.01	1.09	0.64	1.54
171.swim	1.00	1.04	1.08	0.82	1.39
172.mgrid	1.00	1.00	1.10	0.99	1.51
173.applu	1.00	1.08	1.09	0.56	1.75
177.mesa	1.00	1.00	1.11	1.10	1.72
178.galgel	1.00	1.18	1.75	1.77	2.87
179.art	1.00	1.01	2.66	1.68	3.96
183.quake	1.00	1.01	1.10	0.69	1.72
187.facerec	1.00	1.07	1.19	0.76	1.89
188.amp	1.00	1.01	1.38	1.46	2.15
189.lucas	1.00	1.13	1.09	1.00	1.49
191.fma3d	1.00	1.04	1.08	0.85	1.51
200.sixtrack	1.00	1.01	1.17	1.21	1.81
301.apsi	1.00	1.02	1.10	1.76	1.63
SPECfp2000	1.00	1.04	1.23	1.13	1.84

Tabelle 3: SPECfp2000 Werte relativ zu Itanium 2 (900 MHz)

System:	HP rx2600	Intel	Intel	AMD	IBM p655	Blade2000
Prozessor:	Itanium 2	Pentium 4	Pent. 4EE	Athl. FX-51	Power4+	US III
Taktrate:	1.5 GHz	3.2 GHz	3.2 GHz	2.2 GHz	1.7 GHz	1.2 GHz
168.wupwise	1466	1755	1745	1590	2135	959
171.swim	4136	1882	1914	2220	2423	2659
172.mgrid	2503	1238	1323	1216	1214	706
173.applu	3469	1289	1318	1202	1448	956
177.mesa	1126	1324	1323	1579	1024	735
178.galgel	4225	1860	2606	2291	4697	2374
179.art	6514	925	2374	1739	2304	11077
183.quake	2982	1625	1653	1352	2644	1616
187.facerec	1925	1661	1769	1633	1966	1179
188.amp	1413	773	1266	1353	1022	651
189.lucas	1774	1578	1611	1459	2005	716
191.fma3d	1091	1312	1330	1315	1315	547
200.sixtrack	1402	594	606	601	741	454
301.apsi	1024	890	1205	1249	1341	648
SPECfp2000	2119	1267	1494	1423	1678	1118

Tabelle 4: SPECfp2000 Werte einiger Rechnersysteme

lich) übertroffen. Ein extremes Beispiel ist das Programm 179.art, bei dem ein Sun Blade2000 System fast doppelt so schnell ist wie die HP rx2600, wobei die rx2600 wiederum ein Mehrfaches schneller ist als die restliche Konkurrenz.

Der Pentium 4EE Prozessor hat im Gegensatz zum Pentium 4 Prozessor zusätzlich einen on-chip L3 Cache von 2 MB, der einige Benchmark-Programme (beispielsweise 179.art) deutlich beschleunigt. Die IBM p655 pro-

fitiert beim SPECfp2000 enorm vom 128 MB großen L3 Cache, den sich im Normalbetrieb 8 Prozessoren teilen müssen; gibt es allerdings nur einen aktiven Prozess, so kann dieser den ganzen L3 Cache für sich allein nutzen. Programme wie 189.facerec (mit einem Hauptspeicherbedarf von etwa 16 MB) profitieren davon sehr deutlich.

Benchmark-Programme wie der SPECfp2000 zeigen, wie gut (oder schlecht) ein Rechnersystem für die im Benchmark vertretenen Programme geeignet ist. Die ein-

zelen Applikationen haben teilweise deutlich unterschiedliche Anforderungen an die Rechnersysteme; einzelne Werte wie ein SPECfp2000 können die Leistungsfähigkeit eines Computersystems immer nur sehr vereinfacht und nur unter den zugrunde liegenden Annahmen des jeweiligen Benchmarks darstellen. Bei der Auswahl eines geeigneten Rechnersystems für eine bestimmte Applikation können Benchmark-Werte hilfreich sein; als alleinige Entscheidungsgrundlage sind sie nur selten geeignet.

SPECfp_rate2000

SPECint2000 und SPECfp2000 sind nur zur Bewertung der Einzel-Prozessor-Leistung geeignet; für die Bewertung der Durchsatz-Leistung von Mehr-Prozessor-Systemen werden der SPECint_rate2000 und der SPECfp_rate2000 (jeweils wieder als *base* und *peak* Varianten) herangezogen. Bei der Durchsatzmessung werden auf einem n -Prozessor System genau n Kopien des jeweiligen Benchmark-Programmes gestartet und deren Laufzeit gemessen. Die Laufzeiten der einzelnen Benchmark-Programme werden in Relation zu denen des Referenzsystems (Sun Ultra 5/10) gesetzt und gemittelt. Bei einem System, das optimal skaliert, führt eine Verdoppelung der Anzahl der Prozessoren zu einer Verdoppelung des SPECint_rate2000 bzw. SPECfp_rate2000 Wertes (oder anders ausgedrückt: die Laufzeit der Benchmark-Programme ist unabhängig von der Anzahl der Prozessoren).

Die SPECfp_rate2000 Werte in Tabelle 5 stammen von einer HP rx5670, die mit ein bis vier Itanium 2 Prozessoren (1.5 GHz) bestückt sein kann.

Anzahl CPUs:	Laufzeit [s]			Faktor		
	1	2	4	1	2	4
168.wupwise	112.0	120.0	129.0	1.00	1.07	1.15
171.swim	73.8	135.0	273.0	1.00	1.83	3.70
172.mgrid	71.8	117.0	225.0	1.00	1.63	3.13
173.applu	61.7	66.1	101.0	1.00	1.07	1.64
177.mesa	122.0	122.0	122.0	1.00	1.00	1.00
178.galgel	68.3	68.4	69.0	1.00	1.00	1.01
179.art	39.0	39.7	39.7	1.00	1.02	1.02
183.quake	44.6	57.9	108.0	1.00	1.30	2.42
187.facerec	97.0	106.0	124.0	1.00	1.09	1.28
188.amp	155.0	155.0	156.0	1.00	1.00	1.01
189.lucas	114.0	148.0	266.0	1.00	1.30	2.33
191.fma3d	199.0	210.0	251.0	1.00	1.06	1.26
200.sixtrack	80.0	80.0	80.4	1.00	1.00	1.01
301.apsi	260.0	263.0	285.0	1.00	1.01	1.10
SPECfp_rate2000:	24.5	42.6	66.4			

Tabelle 5: Absolute und relative Laufzeiten des SPECfp_rate2000 auf einem HP rx5670

Das Benchmark-Programm 171.swim hat hohe Anforderungen an die Speicherbandbreite des betreffenden Systems. Bei der HP rx5670 verbraucht bereits eine einzige Instanz dieses Programmes einen Großteil der ver-

fügbaren Speicherbandbreite, sodass bei zwei Prozessoren die Laufzeit um den Faktor 1.83, und bei vier Prozessoren die Laufzeit um den Faktor 3.7 ansteigt. Viele Anwendungen im technisch-naturwissenschaftlichen Bereich haben ähnliche Anforderungen, beispielsweise das an der TU Wien entwickelte Programmpaket WIEN. Für derartige Applikationen scheint dieses System nicht geeignet zu sein. (In diesen Fall hätte ein 4-Prozessor System nur eine marginal bessere Durchsatzleistung als das entsprechende System mit nur einem Prozessor.) Bei Applikationen, die vollständig im Cache ablaufen (wie 179.art) oder nur selten Zugriffe auf den Hauptspeicher benötigen, mag eine Konfiguration dieses Systems mit vier Prozessoren sinnvoll sein (sofern man gewillt ist, den Preis von mehr als 100 000 Euro in Kauf zu nehmen).

WIEN

WIEN ist ein umfangreiches Programmsystem aus dem Bereich der theoretischen Chemie zur Berechnung von elektronischen Eigenschaften von Festkörpern nach der FP-LAPW Methode (siehe Blaha et al. [1]), mit dem sehr genaue Lösungen der Gleichungen der Dichtefunktionaltheorie berechnet werden können.

LAPW1 ist Teil von WIEN und beinhaltet der Lösung eines verallgemeinerten Eigenwertproblems, wodurch dieses Programm nicht nur sehr rechenintensiv ist, sondern auch hohe Anforderungen an die Speicherbandbreite des Rechnersystems stellt. Die Laufzeiten für einen konkreten Datensatz sind in Tabelle 6 zusammengefasst.

Die numerisch intensiven Berechnungen sind in die BLAS Bibliothek ausgelagert. Dies ist eine Sammlung grundlegender mathematischer Operationen (beispielsweise Multiplikation zweier Matrizen). Für eine optimale Laufzeit ist in der Regel die Verwendung hoch optimierter BLAS Bibliotheken anzuraten. Die MKL (Math Kernel Library) von Intel ist eine derartige Bibliothek. Ist für ein bestimmtes Computersystem keine vom Hersteller optimierte BLAS Bibliothek vorhanden, steht über NETLIB (www.netlib.org) eine portable, aber im Allgemeinen nicht sehr effiziente Fortran 77 Referenzimplementierung zur Verfügung.

Auf dem Pentium 4 System bringt die Verwendung der MKL von Intel deutliche Vorteile gegenüber der Fortran 77 Referenzimplementierung. Die neueren Versionen des Intel Compilers und der MKL bringen nur noch geringfügige Verbesserungen.

Ein völlig anderes Bild bietet das Itanium 2 System; die extremen Laufzeitunterschiede zwischen den beiden Versionen der MKL belegen den teilweise fehlenden Support bei der Einführung des Itanium 2 Prozessors. Die Laufzeiten unter HPUX belegen, dass auch weiterhin noch Verbesserungen der Intel Compiler möglich sein sollten.

Rechnersystem	Prozessor	Betriebssystem	Compiler	BLAS	Laufzeit
HP rx2600	Itanium 2 900 MHz	Redhat AS 2.1	Intel 7.0	MKL 5.2	3213
		Redhat AS 2.1	Intel 7.0	Netlib	1402
		Redhat AS 2.1	Intel 7.1	MKL 6.0	257
		HPUX 11i	HP	MLIB	225
PC, ASUS P4T533	Pentium 4 2.8 GHz	Redhat 8.0	Intel 7.0	MKL 5.2	210
		Redhat 8.0	Intel 7.1	MKL 6.0	194
		Redhat 8.0	Intel 7.1	Netlib	577

Tabelle 6: Laufzeiten von LAPW1 in Abhängigkeit von Betriebssystem und Compiler

CFD Applikationen

Bei Einführung des Itanium Prozessors war de facto keine Applikations-Software für diese Plattform erhältlich. Mittlerweile gibt es von vielen Anbietern auch Versionen für Itanium-basierte Systeme (sowohl unter HPUX als auch unter 64-Bit Linux).

Am ZID steht ein Applikationsserver für Strömungsdynamik und Finite Elemente zur Verfügung (www.zserv.tuwien.ac.at/sc/). Die Hardware besteht aus 10 Compaq ES45 Systemen mit jeweils 4 Alpha 21264C Prozessoren mit 1 GHz. Als Vergleichssystem diente eine HP rx2600 mit zwei Itanium 2 Prozessoren mit 900 MHz.

Produkt	Testfall	Laufzeit [s]	
		ES45	rx2600
Fluent	big	927	1188
	small	149	186
Ansys	big	10980	13470
	small	820	1230
Cfx5	big	36112	46250
	small	472	544

Tabelle 7: Laufzeiten einiger CFD Applikationen

Beide Systeme sind mit nicht mehr ganz aktuellen Prozessoren ausgestattet. Bei allen drei Applikation ist der Alpha Prozessor um etwa 20 – 40 % schneller als der Itanium 2 Prozessor. Ein Vergleich der derzeit jeweils leistungsfähigsten verfügbaren Prozessoren würde wahrscheinlich zu Gunsten des Itanium 2 Prozessors ausgehen.

Resümee

Der Itanium 2 ist ein sehr leistungsfähiger Prozessor, der überall dort seine Berechtigung findet, wo man mit den Beschränkungen der IA32 Architektur nicht leben kann oder will. Im Bereich großer SMP Systeme beginnen Itanium-basierte System den etablierten Server-

systemen Konkurrenz zu machen: HP bietet mit der Superdome Systeme mit bis zu 64 Prozessoren; SGI bietet mit der Altix Systeme mit bis zu 128 Prozessoren (eines davon ist an der Universität Linz installiert). Zudem können mehrere Altix Systeme zu einem Super-Cluster verbunden werden, wobei jeder Prozessor auf den gesamten Hauptspeicher aller beteiligten Systeme zugreifen kann (www.sgi.com/servers/altix).

Die effiziente Portierung einer Applikation auf die Itanium 2 Plattform kann sehr zeitaufwendig sein, speziell wenn es sich um C/C++ Code handelt. Intel übernimmt zwar laufend Features vom GNU C Compiler in seine Compiler, unter Linux/gcc entwickelte Applikationen müssen aber in den meisten Fällen für die Verwendung der Intel Compiler adaptiert werden. Auf Itanium Systemen sind die Intel Compiler aus Gründen der Effizienz dem GNU C Compiler vorzuziehen; auf IA32 Systemen sind die beiden Compiler mittlerweile etwa gleichwertig.

Wenn die Beschränkungen der IA32 Architektur (Adressraum mit 4 GB limitiert) nicht zum Tragen kommen, bieten IA32 Systeme ein deutlich besseres Preis/Leistungsverhältnis. (Für den *high-end* Itanium 2 Prozessor mit 1.5 GHz und 6 MB Level 3 Cache sind ca. 10 000 Euro Listenpreis zu kalkulieren.) Und mit den Opteron bzw. Athlon64 Prozessoren ist durch deren Kompatibilität mit der IA32 Architektur zudem ein wesentlich sanfterer Einstieg in die 64-Bit Welt möglich.

Am ZID wurde ein Evaluierungsserver für den Itanium 2 Prozessor eingerichtet; weitere Informationen findet man unter www.zid.tuwien.ac.at/zserv/systeme/titan.html.

Literatur

- [1] P. Blaha, K. Schwarz, P. Sorantin, S. B. Trickey: *Full-Potential, Linearized Augmented Plane Wave Programs for Crystalline Systems*. Comp. Phys. Commun. 59 (1990), pp. 399–415.

Erste Windows 2003 Server Erfahrungen eines ungeschulten Administrators

Albert Blauensteiner

Im Folgenden sollen einige erste Eindrücke und Erfahrungen mit dem neuen Server-Betriebssystem Windows 2003 dargelegt werden.

Zunächst stellt sich immer die grundsätzliche Frage, warum man ein neues Serverbetriebssystem überhaupt aufsetzen soll. Nur schwer lässt sich von vornherein abschätzen, ob die Risiken, die ein neues System mit den noch nicht vorhandenen Erfahrungen die Vorteile der zahlreichen Neuversprechungen und Verbesserungen aufwiegen. Sicherlich ist es auch ein Unterschied, ob man ein System für eine neue Anwendung erstmals neu konzipiert oder ob man in einem bestehenden Umfeld mit einem mehr oder weniger zufrieden laufenden System ein Upgrade vornehmen will. Letzteres war bei mir der Fall und die Motivation zu einem Upgrade von Windows 2000 Server auf Windows 2003 Server war nicht technisch begründet sondern darin, mir auf Grund eines Hardwareumstieges konkret ein Bild des neuen Serverbetriebssystems zu machen, um dessen Einsatz auf dem Campus ganz konkret beurteilen zu können.

Grundsätzlich empfiehlt es sich, wenn man es sich betrieblich leisten kann und einen Tag Betriebspause einlegen kann, das System nicht upzugraden sondern neu zu installieren. Damit erspart man sich meistens eine ganze Reihe von Folgeproblemen, die die Neueinstellung der benutzerspezifischen Eigenschaften bei weitem aufwiegen. Außerdem wird viel unnötiger Ballast, der sich im Laufe der Jahre in der Registry ansammelt, abgeworfen.

Die Installation von Windows 2003 Server ist völlig problemlos. Das System ist optisch Windows XP vollkommen angeglichen und ebenso wie XP auf NT Technologie basierend. Nach der Installation ist das System wie eine Desktop Workstation installierbar, alle Servereigenschaften sind *disabled* oder noch nicht installiert, was ein positiver Ansatz ist, nicht zu letzt in Hinblick auf Security.

Beim Einrichten einer Domain bzw. spezifischer Server – wie bei mir dem Exchange 2003 Server – habe ich den Weg gewählt, die Systemwartung der Abteilung Standardsoftware an der Technischen Universität Wien in Anspruch zu nehmen und einen entsprechenden Call zur Unterstützung abzusetzen. Das empfiehlt sich grundsätzlich, wenn man – wie es bei mir der Fall ist – ein typischer, nicht geschulter Systemadministrator ist, der aus organisatorischen Gründen einen Server zu betreuen hat, aber keine speziellen Schulungen in Anspruch genommen hat. Das fiel mir „zufällig“ umso leichter, da ich als Leiter der Abteilung Standardsoftware um die Qualität der Plattformunterstützung Bescheid weiß und die Effizienz dieses Einsatzes schätze. Prompt bekam ich auch erstklassige Unterstützung, wobei das Aufsetzen der Domain und der einzelnen Server keinerlei Schwierigkeiten bereitete, wenngleich die konkreten Arbeiten zum Teil kompliziert und nicht übersichtlich sind und man sich vor diesen Arbeiten genau im Klaren sein sollte, was für Funktionen man mit dem Server plant und wie das organisatorische und betriebliche Umfeld gestaltet werden soll. Man sollte sich auch vom Active Directory Service nicht einschüchtern lassen. Wenn man sich damit nicht weiter beschäftigen will, so hat man nach der Installation tatsächlich weiter nichts damit zu tun. User lassen sich ganz leicht auch in Gruppen strukturieren. Trees und Forrests können in Windows 2003 leicht und viel besser als in Windows 2000 gemanagt werden.

Unverständlich bleibt, warum Microsoft die Produkte Windows 2003 Server, Exchange 2003 Server und Office 2003 doch zu so ziemlich verschiedenen Zeitpunkten auf den Markt bringt, wo gerade diese Kombination von einander abhängig ist und auch nur zusammen sinnvoll installiert werden kann. In diesem Zusammenhang möchte

ich gleich erwähnen, dass Office 2003 bis zum Zeitpunkt meiner Installation noch immer nur als Beta Version verfügbar war. Das brachte mir das Problem, dass Outlook 2003, so nett es auch aussieht, völlig unbrauchbar war, weil bereits Eigenschaften wie Mail Forward nicht funktionierten. Nach wie vor unverständlich ist es mir, dass bei neuen Office Versionen nach wie vor gleiche Einstellungen in den Optionsmenüs völlig unterschiedlich aufzufinden sind und gehandhabt werden wie z.B. Pfadeinstellungen etc. Nett ist in Outlook 2003, dass auch endlich das Newsservice direkt eingebettet ist. Die Synchronisation mit meinem PDA funktioniert problemlos. Die Mails werden zum Teil neu und recht übersichtlich strukturiert dargestellt.

Es ist auch kein Problem, alle gängigen Applikationen wie Acrobat in den neuesten Versionen unter Windows 2003 Server zu installieren. Selbst die Brennsoftware Nero funktioniert in der neuesten Version 6 problemlos. Meinen einzigen Blue Screen habe ich erhalten, als ich die vorher erwähnte Office 2003 Beta 2 Version auf Empfehlung von Microsoft mit einem am Netz verfügbaren Patch updaten wollte.

Es sieht auch so aus, als ob alle gängigen Peripheriegeräte und Devices problemlos mit den XP Treibern funktionieren. Unrühmliche Ausnahme ist Logitech, sowohl Mäuse als auch Kameras werden unter Windows 2003 Server nicht unterstützt. Dazu erteilte mir Logitech die Auskunft, dass sie aus strategischen Gründen keine Serversysteme (auch Linux) unterstützen und auch nicht vorhaben, diese in Zukunft zu unterstützen. Selbstverständlich funktionieren aber die Standarddriver auch für Logitech Mäuse. Daher habe ich mir eine Microsoft Maus angeschafft, hier kann ich jetzt in gewohnter Weise auch meine mittlere Maustaste belegen. Nebenbei habe ich dabei festgestellt, dass diese Maus viel sensitiver reagiert und viel handlicher ist, was dazu führt, dass ich dieser Maus in Zukunft einen Vorzug gegenüber Logitech einräumen möchte. Sicherlich freut sich auch die Firma Logitech, dass ich meinen Server nicht mehr mit ihren Mäusen „verunreinigen“ muss.

Auch der Internet Information Server wird glücklicherweise so installiert, dass keine sicherheitsspezifischen Probleme in der Standardinstallation offen sind. Übrigens lässt sich leicht das ganze Desktop Erscheinungsbild so einstellen, wie man es von Windows 2000 gewohnt war. So wird man nicht von der XP Modernität „belästigt“.

Zu empfehlen ist das interne Microsoft Backup, weil man auf diese Weise ganz gezielt alle kritischen Systemdateienbestände retten kann, auch wenn sie selbst im System zum Zeitpunkt des Backups verwendet werden. Problemlos unterstützt werden auch DVD Drives, ebenso Videos. Mit dem Einsatz des Terminal Servers können leicht andere User Zugang zum Windows 2003 Server erhalten, die Performance ist dabei sehr gut. Zum Shut Down benötigt der Server über 10 Minuten, eine doch ungewöhnlich lange Zeit, allerdings sollte das Herunterfahren des Rechners hier die Ausnahme darstellen. Mit der Hyperthreading Technologie des Pentium 4,3 GHz werden zwei virtuelle Prozessoren deutlich merkbar zur Lastverteilung eingesetzt.

Übrigens ist Java Virtual Machine nicht verfügbar, dies entspricht der neuen Microsoft Vorgangsweise, ab sofort die Betriebssysteme aufgrund des Rechtsstreits mit Sun damit nicht mehr auszurüsten. Java VM kann man aber ohne Probleme von SUN beziehen und installieren. Diese Konfiguration ist allerdings nur dann für einen Windows 2003 Server Benutzer umständlich, wenn man sich – wie ich – auf dem gleichen System als User einrichtet, um einen Arbeitsplatz zu sparen.

Nach einiger Zeit habe ich mir die Norton Internet Security installiert, die an sich nicht für Serversysteme vorgesehen ist. Es gab dabei aber keinerlei Schwierigkeiten und außerdem war es recht einfach, die Einstellungen auf die notwendigen Dienste anzupassen. Das betraf das User Logon, das Webservice, das Filesharing so wie einige externe Dienste wie das Backup von außen. Aufpassen muss man nur beim Startup: Derzeit ist es bei meinem System so, dass ich händisch Netlogon starten muss, danach alle Exchange Dienste und erst danach den Firewall.



Neue Studentensoftware
sts.tuwien.ac.at/sss/



Neue Firewall-Lösung für die TU-Institute auf Linux-Basis

Walter Selos

Die bereits am ZID existierenden bewährten Lösungen, die mit einer Diskette das Auslangen finden, haben den Nachteil, dass auf der Diskette sowohl die Systemsoftware wie auch die Konfigurationsdateien untergebracht werden müssen. Das kann – vor allem bei sehr vielen Firewall-Regeln – zu Platzproblemen führen. Als Abhilfe wird hier eine wesentlich flexiblere Lösung – basierend auf einer CD – vorgestellt. Auf der dennoch notwendigen Diskette sind nur noch die Konfigurationsdateien sowie einige dazu notwendige Scripts vorhanden.

Für eine weitere Beschreibung dieser Lösung möchte ich nochmals deren Ziel in Erinnerung rufen, nämlich einen einfachen Paketfilter zur Verfügung zu stellen, der bei der Inbetriebnahme keine Konfigurationsmaßnahmen an den involvierten Computern erfordert. Im Falle eines Ausfalls des Gerätes, kann man (allerdings ungeschützt) weiter arbeiten, indem das Gerät durch ein ausgekreuztes Patchkabel ersetzt wird, ebenfalls ohne weitere Konfigurationsmaßnahmen. (Das kann allerdings auf einigen Switches der TU Schwierigkeiten machen, daher bitte vorher die Abt. Kommunikation kontaktieren.) Voraussetzung hierfür ist, dass die hinter dem Firewall liegenden (zu schützenden) Computer zu einem VLAN oder mittels Switches so zusammengefasst werden, dass deren gesamter Netzwerkverkehr durch ein einziges Kabel geführt wird. Dieses kann dann durch den Firewall ersetzt werden. Dazu ist es notwendig, mit dem ZID, Abt. Kommunikation, Kontakt aufzunehmen.

Diese Firewall-Lösung ist schon an einigen Stellen längere Zeit im Einsatz und läuft sehr stabil. Da sowohl in der Planungsphase als auch bei der Aufstellung und Konfiguration immer wieder spezifische Fragen auftauchen, möchte ich in den nächsten Zeilen das Konzept genauer betrachten und einige Details und Tipps bekannt geben, die aufgrund der bisherigen Betriebserfahrung für Aufstellung, Konfiguration und Betrieb hilfreich sein werden.

Wie funktioniert dieser Firewall ?

Es wird, wie bereits bei der letzten Disketten-Lösung, *Proxy-Arp* verwendet. Dies hat den Vorteil, mit Stan-

dardkomponenten von Linux auszukommen, um ohne zusätzliche Patches eine „Pseudo-Bridge“ zu realisieren, allerdings nur für IP-Protokolle.

Zum weiteren Verständnis ist es notwendig, einige Worte über das *Arp-Protokoll* zu verlieren: Sind mehrere Computer mit Ethernet-Schnittstellen zu einem LAN verbunden, wird der Netzwerkverkehr auf der untersten Ebene mit dem Ethernet-Protokoll bewerkstelligt. Die Adressierung der einzelnen Rechner erfolgt über die so genannte MAC-Adresse, eine weltweit eindeutige Adresse für jede Ethernet-Karte. Da wir aber IP-Protokolle (tcp, udp, icmp, snmp, gre ...) verwenden, haben wir mittels Konfiguration der Firewall-Software jedem Rechner eine eindeutige IP-Adresse vergeben. Wenn wir einen anderen Rechner in unserem LAN über seinen DNS-Namen ansprechen, gibt uns der Nameserver der TU die dazugehörige IP-Adresse *xxxx* zurück. Der Firewall-Rechner macht nun ein Broadcast auf das ganze LAN mit der Frage „Wer hat die IP-Adresse *xxxx* ?“.

Der Rechner mit dieser Adresse gibt nun seine MAC-Adresse zurück, womit die Verbindung mittels des Ethernet-Protokolls aufgebaut werden kann. Diese wird temporär im so genannten *arp-cache* abgespeichert, welchen Sie sich jederzeit, sowohl unter Unix/Linux wie auch unter Windows ansehen können (der Befehl dazu heißt: *arp*).

Erklärung der Funktionsweise von Proxy-Arp:

Nachdem im Linux-Kernel (/proc - Filesystem) *ip_forwarding* sowie *proxy_arp* für beide Interfaces aktiviert wurden (siehe die echo „1“ > /proc/... - Einträge in der Script-Datei „fwrules“), müssen nun für jeden am Insi-

de-Interface angeschlossenen Rechner (das sind die zu schützenden) statische Routen eingetragen werden (dies macht das Script „fwrules“ automatisch, wenn man diese Rechner in eine Datei „inside_hosts“ auf der Diskette einträgt).

Wenn nun eine Verbindung zwischen innen und außen hergestellt wird, wird die durch das ARP-Protokoll erhaltene MAC-Adresse durch die MAC-Adresse des zweiten Interfaces des Firewall-Rechners ersetzt. Die Rücksubstitution kann der Firewall mittels der eingetragenen statischen Routen bewerkstelligen.

So sieht man im *arp-cache* eines Rechners innerhalb des Firewalls alle außerhalb liegenden IP-Adressen mit der selben MAC-Adresse (nämlich der des Inside-Interfaces des Firewalls). Ebenso sind im *arp-cache* eines außerhalb des Firewalls liegenden Rechners alle innen liegenden IP-Adressen mit der MAC-Adresse des Outside-Interfaces des Firewalls zu sehen.

Man hat dadurch die Funktion einer Ethernet-Bridge, die allerdings nur IP-Pakete durchlässt. Über die mittels *iptables* gefilterte *FORWARD-chain* lassen sich Firewall-Regeln definieren (siehe Datei „fwrules“).

Das heißt auch, dass man beim Anschluss der Rechner hinter dem Firewall mitunter auf den Timeout der ARP-Caches warten muss (besonders beim Ändern der Konfiguration zwischen Firewall und ausgekreuztem Patchkabel).

Um dieses Warten zu verkürzen und aus anderen Gründen, welche mit der ausfallsicheren Konfiguration vieler unserer Router zu tun haben, wird von einem Programm (*broadarp*) ein ARP-Broadcast beim Startup des Firewalls durchgeführt, welches alle im „inside_hosts“-File eingetragenen Rechner mit der MAC-Adresse des Firewalls nach außen bekannt gibt.

Wie man aus dem Konzept erkennen kann, ist es nicht nur möglich, ein gesamtes Subnetz hinter den Firewall zu positionieren, sondern auch nur Teile davon.

Erläuterungen zum Linux-Teil des Firewalls (für UNIX-Eingeweihte)

Es wurde, basierend auf Mandrake 9.0 eine bootfähige CD zusammengestellt. Beim Bootvorgang werden die beschreibbaren Dateien (z.B. */etc/* /home/* /tmp/* /var/log/**) auf einer RAM-Disk abgelegt.

Das System startet dann im Runlevel 2. Als erstes Script in diesem Runlevel wird die Datei „config“ aufgerufen. Diese sieht nach, ob eine FAT-Diskette am Mountpoint */config_dir* gemountet ist und diese eine Datei „fw01“ beinhaltet. Wenn ja, wird die Datei „config“ auf der Diskette gesucht und als Script gestartet. Da kann man theoretisch hineinschreiben, was man will, was bedeutet, dass man es hier mit einer sehr allgemeinen Schnittstelle zu tun hat und man keineswegs nur auf die Funktion als Firewall eingeschränkt ist, der Phantasie sind hier keine Grenzen gesetzt.

So habe ich schon als Anregung für andere Verwendungsmöglichkeiten auf der CD im Unterverzeichnis */samples* Beispiel-Disketten nicht nur für *Proxy-Arp*, son-

dern auch für die Verwendung IP-Masquerading, Adsl-Router und ISDN-Router (ohne Funktionsgarantie, obwohl die alle schon einmal gelaufen sind ...) abgelegt.

Es gibt ziemlich vollständige Manualpages auf der CD, einen *vi* (die nicht *vi*-Kundigen können den Editor vom „mc“ – einem Norton-Commander-Nachbau für Linux – verwenden, dennoch sollten Unix-Unkundige sehr vorsichtig ans Werk gehen ...).

Man könnte auch (aber bitte nur kurzfristig, für Wartungszwecke!) einen *sshd* starten, man kann einen *syslogd* starten, aber auch nur zum Fehlersuchen, weil die RAM-Disk nicht allzu groß ist, oder längerfristig, aber dann übers Netz auf eine andere Unix/Linux-Maschine (*syslog.conf* auf die Diskette bringen, editieren und über ein vorhandenes Script, z.B. „fwrules“ auf */etc* kopieren und danach den *syslogd* starten).

Ebenso kann man sich mit *ssh* auf andere Maschinen einloggen (gut für Testzwecke) und damit auch Dateien (z.B. Konfigurationsdateien) auf einer anderen Maschine abspeichern.

Ein Vorteil dieser Lösung: Es kann kein Hacker (sollte, was allerdings sehr unwahrscheinlich ist, doch einer reinkommen) sich mit einem Rootkit breit machen (die Diskette sollte ja schreibgeschützt sein und die RAM-Disk ist nach einem Neustart auch garantiert Rootkit-frei!).

Inbetriebnahme

Voraussetzungen:

- PC mit i586-Technologie, PCI-Bus
- RAM \geq 64 MB (je größer, umso mehr Betriebssicherheit, da es ja kein Swap-space aktiviert ist)
- CPU > 300 MHz
- 2 Ethernetkarten (Es werden die meisten unterstützt, auf der CD auf */samples/drivers.txt* sind die verfügbaren Kernelmodule aufgelistet)
- 1 CD-Laufwerk (IDE !) und ein Diskettenlaufwerk
- Ein für diesen Zweck vorbereitetes Netzwerk.
- Die Firewall-CD (erhältlich auf: linux.tuwien.ac.at/fwiso/isofw.iso, (man kann sich auch den Inhalt der CD auf diesem Server ansehen) und eine FAT-formatierte Diskette
- Am PC das BIOS-Setup so einstellen, dass von der CD gebootet wird

Jetzt kann von der Firewall CD gebootet werden.

Wenn Sie beim Login-Prompt als *fwadmin* (Passwort: *firewall*, Sie bekommen root-Rechte) einloggen, werden die Netzwerkkarten am pci-Bus gesucht und ausgeschrieben. Das erleichtert Ihnen die Suche nach den nötigen Kernelmodulen.

Dann wird empfohlen, das Script „makefloppy“ aufzurufen. Im Auswahlmene wählen Sie dann „proxy-arp“ aus und ändern die Passwörter für root und fwadmin.

Es werden dann die Beispiel-Dateien von */samples/proxy-arp* auf die Diskette geschrieben, ebenso die neuen Dateien */etc/passwd* und */etc/shadow*.

Die Diskette ist nun auf `/config_dir` gemountet und Sie müssen nun die beiden relevanten Konfigurationsdateien „myconfig“ und „fwrules“ editieren und alle innenliegenden Rechner in die Datei „inside_hosts“ eintragen (am besten mit der IP-Adresse).

Einige Tipps

- Geben Sie dem Inside-Interface eine private Adresse aus dem Subnetz 192.168.1.0, also z. B. 192.168.1.1.
- Identifizieren Sie die Drivermodule für Ihre Netzwerkkarten, siehe login als „fwadmin“. Wenn Sie zwei gleiche Karten haben, kann es etwas schwierig sein, das außenliegende vom innenliegenden Interface zu unterscheiden. Dazu müssen Sie, nach getaner Konfiguration der Datei „myconfig“ und Neustart versuchen, Ihren Router zu „pingen“ und das nach außen führende Netzwerkkabel solange umzustecken, bis der Router antwortet. Wichtig: Markieren Sie die zusammengehörigen Steckdosen und Interfacebuchsen mit „Innen“ und „Außen“, damit Sie nach etwaigem temporärem Abbau des Gerätes nicht wieder experimentieren müssen !
- In „fwrules“ ist auf der Beispiel-Diskette eine Standardkonfiguration, die es erlaubt, dass von innen nach außen jeder Verbindungsaufbau möglich ist, von außen nach innen jedoch keiner, außer „ping“. TCP-Pakete, die eine Verbindung von außen initiieren, können in den Filterregeln mit `-sync` separat behandelt werden.
- Wollen Sie einige Server für bestimmte Ports zugänglich machen, müssen Sie den Namen „myserver“ mit der IP-Adresse Ihres Servers substituieren (der DNS-Name wäre auch möglich, nur hängt dann die ganze Sache, wenn der Nameserver nicht erreichbar ist, dasselbe gilt auch für die Datei `inside_hosts`) bzw. bei den bereits als Kommentar eingetragenen Beispielszeilen das Kommentarzeichen löschen.
- Wenn Ihnen nicht wirklich klar ist, was hier zu tun ist, wäre es nicht im Sinn der Sicherheit Ihres zu schützenden Netzwerks, bedenkenlos zu experimentieren. Sie können die Unterstützung des ZID, Abt. Standardsoftware im Rahmen eines sehr günstigen Wartungsabkommens in Anspruch nehmen.
Für Fragen zur Planung oder kurze Fragen zur Konfiguration können Sie uns natürlich auch ohne Wartungsabkommen kontaktieren. (Siehe: Fernunterstützung für Arbeitsplatzrechner sts.tuwien.ac.at/pss/, im Fall einer Firewall-Installation kommen wir dennoch vor Ort).
- Lesen Sie sich bitte gut die Manualpages und HOWTOS für den Packetfilter „iptables“ durch, das hilft Ihnen auch, die Beispiele in der „fwrules“-Datei zu verstehen.
- Machen Sie zuerst eine einfache Konfiguration und testen Sie sie einige Zeit aus. Günstig ist es, zuerst Tests zu

machen mit deaktivierten Firewall-Regeln, das geschieht durch den Befehl `iptables -F`. Dann müsste alles so funktionieren wie zuvor mit dem ausgekreuzten Kabel.

- Vergessen Sie nicht, nach dem Editieren der Diskette zumindest ein `sync` abzusetzen, wenn nicht ein `umount` zu machen, da sonst der Inhalt zerstört sein kann. Nach erfolgter (und getesteter) Konfiguration starten sie den Firewall neu mit schreibgeschützter Diskette.
- Wenn Sie etwas auf der Diskette nacheditieren wollen, gehen sie so vor: `umount /config_dir`, dann den Schreibschutz der Diskette deaktivieren und wieder mit `mount -t vfat /dev/fd0 /config_dir` mounten. Nach den Änderungen `umount /config_dir`, Schreibschutz aktivieren und neu starten.
- Wenn Sie nur die Filterregeln oder die `inside_hosts` editiert haben, und das ohne Neustart einmal testen wollen, löschen Sie zuerst die Filterregeln mit dem Kommando `iptables -F` und starten Sie dann nochmals das Script `/config_dir/fwrules`.
- Testen Sie Ihre Firewall-Regeln, indem Sie erlaubten und nicht erlaubten Netzwerkverkehr verursachen und die Reaktion des Firewalls verifizieren. Je mehr Sie hier testen, umso sicherer sind Sie vor unliebsamen Überraschungen, die sich oft viel später auswirken können. Achten Sie dabei besonders auf weniger alltägliche potentielle Probleme, wie z.B. Zugriffsmöglichkeiten auf Lizenzserver für Applikationen, die Sie eher selten brauchen (wenn der Firewalladministrator auf Urlaub ist, braucht sie sicher jemand, und natürlich ganz dringend !). Diese Lizenzserver benötigen oft das Recht auf einen Verbindungsaufbau von außen um „challenge-response“-Sequenzen durchführen zu können.
- Machen Sie eine Kopie der Diskette (geht auch auf Windows, da es sich um VFAT handelt !) und kopieren Sie Ihre editierten Konfigurationsdateien (also: `myconfig` `fwrules` und `inside_hosts`) auf einen anderen Rechner. Es ist schon (bei den Vorgängerversionen) nach jahrelangem Betrieb vorgekommen, dass die Diskette schadhafte wurde und mangels einer Sicherungskopie die ganze Konfiguration mühevoll neu erstellt werden musste, was längere Betriebsbeeinträchtigungen nach sich ziehen kann.

Links

Download: linux.tuwien.ac.at/Security.html

Advanced Routing Howto: gd.tuwien.ac.at/opsys/linux/LDP/HOWTO/Adv-Routing-HOWTO/

Wartung: sts.tuwien.ac.at/pss/

Wurmattaken

Ingmar Jaitner, Johann Klasek

In diesem Jahr trat weltweit eine der heftigsten Internet-Attacken auf, über die sogar die Presse berichtete. Vor allem der Sobig.F Wurm verbreitete sich im vergangenen August an der TU Wien sehr rasch. Bis Ende September wurden auf den Mail-Bastionsrechnern des ZID etwa 1,5 Millionen verseuchte E-Mails abgefangen. Einschränkend muss man aber sagen, dass nur Windows-Rechner betroffen waren, für Mac- und Linux-User gab es Entwarnung.

W32/Sobig.F

Am 19. August 2003 ab ca. 12 Uhr traten die ersten W32/Sobig.F Wurminfektionen auf Rechnern der TU auf. Zu diesem Zeitpunkt war noch kein Virenupdate für den Virenchecker Cluster verfügbar. Auch die zweite Stufe, der McAfee Virenschanner auf den lokalen Workstations, war bis ca. 16 Uhr nicht geschützt. Der Mail-Bastionsrechner des ZID konnte ab 15 Uhr mit einer Speziallösung gepatcht werden. Vor allem vor dieser Zeit verbreitete sich der Wurm rasch über E-Mails mit gefälschten Absenderadressen und Empfängeradressen, die mitunter vertrauenswürdig wirkten. Die E-Mails haben folgende mögliche Subject-Zeilen:

Re: Thank you!
Thank you!
Your details
Re: Details
Re:Re: My details
Re:Approved
Re:Your application
Re:Wicked screensaver
Re: That movie

Folgende Attachments sind beobachtet worden, die diesen Wurm in sich tragen:

your_document.pif
document_all.pif
thank_you.pif
details.pif
document_9446.pif
application.pif
wicked_scr.scr
movie_0045.pif

Der Wurm braucht die Interaktion eines Benutzers, der diese Attachments öffnet, oder einen E-Mail Client, der Attachments automatisch öffnet. Bei der erfolgreichen Ausführung installiert sich der Wurm selbst als `c:\%windir%\winppr.exe` und erzeugt ebenfalls ein

File `c:\%windir%\winstt32.dat`. Ein Eintrag ist ebenfalls im Run Registry Key vorgenommen worden, sodass das Wurmprogramm beim System Start ausgeführt wird.

Der Key ist in `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run` mit dem Namen `ScanX` mit dem Wert `c:\winnt\winppr.exe /sinc`. Das Programm durchsucht Dateien mit gewissen Extensions (`htm`, `html`, `dbx`, `hlp`, `mht`, `txt`, `wab`) am kompromittierten System nach E-Mail Adressen und nutzt einen eigenen SMTP-Mechanismus, um den Wurm zu verbreiten. Das hatte insofern Folgen für die TU, da SMTP-Verkehr innerhalb der TU ohne zentralen Virenschanner erlaubt ist. Der Wurm nutzt weiters das NTP-Protokoll, um die aktuelle Zeit zu bestimmen. Der Wurm hat ebenfalls Code enthalten, der eine Liste von 20 vorbestimmten IP Adressen an Port 8998/UDP am Freitag und am Sonntag zwischen 19 und 22 Uhr UTC (beginnend um 19 Uhr UTC am 22. August 2003) kontaktiert. Man nimmt an, dass dort eine Lokation ist, die zusätzlichen Code über diesen Kanal überträgt. Die Liste der IP-Adressen ist folgende:

12.158.102.205
12.232.104.221
218.147.164.29
24.197.143.132
24.202.91.43
24.206.75.137
24.210.182.156
24.33.66.38
61.38.187.59
63.250.82.87
65.177.240.194
65.92.186.145
65.92.80.218
65.93.81.59
65.95.193.138
66.131.207.81
67.73.21.6
67.9.241.67
68.38.159.161
68.50.208.96

Der Wurm hat ein programmiertes „Shut Down“ am 10. September 2003, wo er aufhörte, sich zu verbreiten. Alle wichtigen Antivirenhersteller haben mittlerweile Erkennungssignaturen für den Wurm.

W32/Blaster

Der W32/Blaster Wurm nützt eine Schwachstelle in Microsofts DCOM/RPC Interface aus. Wenn er erfolgreich ausgeführt wurde, versucht der Wurm eine Kopie von msblast.exe von dem System, das angegriffen hat, zu laden. Wenn das File geladen ist, arbeitet das kompromitierte System es ab und versucht, weitere Systeme zu verseuchen.

Es wird probiert, zuerst eine Port 135 Session aufzubauen, um den Angriff auszuführen. Port 139 und Port 445 können ebenfalls betroffen sein. Ungewöhnlicher Verkehr zu windowsupdate.com könnte ein Anzeichen für eine Infektion am Netzwerk sein, darum könnte die Überwachung des Netzwerk-Verkehrs nützlich sein.

Das ZID bietet einen eigenen Windows-Update-Server an (sts.tuwien.ac.at/css/ms/MSUS.html), über den automatisch Sicherheitsupdates eingespielt werden können.

Sofortmaßnahmen:

- Physikalisches Abstecken des Rechners
- Den Wurm mit Hilfe des Task Managers löschen. Bekannte Varianten nennen sich msblast.exe, teekids.exe und penis32.exe. Ctrl+alt+del drücken, Taskmanager aufrufen, Prozesse msblast.exe entfernen. End Process + ja beim Warnungsdialog drücken.
- Internet Connection Firewall (eingebaut bei Windows XP) oder eine Personal Firewall installieren.

Wichtig: Danach alle aktuellen Sicherheitspatches anbringen. Den Patch findet man unter www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-026.asp

Ein Removal Tool gibt es unter securityresponse.symantec.com/avcenter/venc/data/w32.blaster.worm.removal.tool.html

W32/Welchia

Ein weiterer Wurm, der uns ein wenig später getroffen hat, ist der W32/Welchia Wurm. Er nutzt dieselbe Schwachstelle aus wie der W32/Blaster:

- er löscht W32/Blaster Artefakte,
- er führt ICMP Scannings durch, um Zielsysteme zu identifizieren

Den Patch zum Schutz findet man auf: www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-026.asp

Ein Removal Tool für den W32/Welchia Wurm befindet sich auf securityresponse.symantec.com/avcenter/venc/data/w32.welchia.worm.removal.tool.html

Der Grund, dass beide Würmer den Computer infizieren können, liegt im RPC Interface, das Buffer Overruns zulässt. *Remote Procedure Call* ist ein Kommunikations-Protokoll, das vom Windows Betriebssystem genutzt wird. RPC stellt einen Interprozesskommunikationsmechanismus zur Verfügung, der einem Programm erlaubt, Code auf einem anderen System auszuführen.

Das Protokoll selbst ist ein Abkömmling des Open Software Foundation RPC Protokolls, aber mit Microsoft Spezifika. Die aufgetretene Lücke hat mit dem Basissystem zum Austausch von Nachrichten via TCP/IP zu tun, auf das sich diverse komplexere Protokolle (wie etwa DCOM) stützen. Der Fehler resultiert aus der inkorrekten Behandlung von schlechtgeformten Nachrichten. Das Interface verwendet DCOM Aktivierungs-Requests, die von Client-Maschinen zum Server gesendet werden. Ein Angreifer, der diese Lücke erfolgreich ausgenutzt hat, kann beliebige Aktionen auf dem System starten, z. B. Programme installieren, Daten anschauen, verändern oder gar neue Accounts mit vollen Privilegien anlegen.

Schlussfolgerungen

Was sind also die Schlussfolgerungen, die ein Benutzer aus diesen vergangenen Internet-Attacken zu ziehen hat?

Auch wenn es Ausnahmesituationen gibt, wo gleich mehrere Sicherheitsstufen versagen, ist und bleibt ein regelmäßiges Patchen nicht nur bei kommerziellen, sondern auch für den privaten Anwender unerlässlich. Natürlich gibt es dabei immer die Gefahr, dass nachher Programme nicht mehr funktionieren, aber ist ein gehacktes System nicht eine größere Gefahr? Auch muss bei den Securitymaßnahmen auch die Waage Security versus Usability im Auge behalten werden.

Der ZID stellt sowohl personelle als auch materielle Ressourcen zur Verfügung, um den Betrieb auf der Universität zu garantieren.

Wo Systemunterstützungs-Wartungsverträge bestehen (sts.tuwien.ac.at/pss/), werden die Viren und Würmer von uns beseitigt und die Rechner gepatcht, in den anderen Fällen geben wir Hinweise zur Sicherung der Systeme.

Aktuelle Informationen zur Viren- und Würmer-Problematik finden sich auf den Webseiten der ZID Security: www.zid.tuwien.ac.at/security/

An dieser Stelle soll wiederum darauf hingewiesen werden, dass selbst von anscheinend vertrauenswürdigen Absendern (diese Information ist in einer E-Mail beliebig fälschbar) Attachments mit Vorsicht zu behandeln sind. Denn auch TUNET-intern kann sich ein Virus/Wurm trotz aller globalen Anti-Viren und Firewall-Vorkehrungen verbreiten. Eine erhöhte Sicherheit erreicht man durch den Einsatz einer Desktop-Antivirensoftware

(siehe Campus-Software), speziell dann, wenn man nicht einfach überprüfen kann, ob das eine oder andere Attachment wirklich verdächtig ist bzw. vom Absender guten Glaubens (aber leider viren- bzw. wurmbefahet) auf den Weg gebracht wurde.

Als verdächtig haben sich immer wieder Attachments mit Dateinamenserweiterungen der Art .exe, .com, .scr, .pif, .doc, .xls, .ppt u.a. herausgestellt, die entweder ein direkt ausführbares Programm oder ein Dokument mit Makrofunktionen enthalten. Als wesentliche Grundvoraussetzung für eine Beurteilung muss allerdings gewährleistet sein, dass das Betriebssystem bzw. die Applikationen wirklich alle Dateierweiterungen darstellen (Explorer) und Attachments obiger Art nicht automatisch von einem Programm zur Ausführung gelangen (Outlook Express älteren Datums).

Im Zweifelsfall hilft hier eventuell auch die direkte (telefonische) Kontaktaufnahme mit dem Absender.

Weiters empfehlen wir, Anti-Viren-Software laufend auf dem aktuellen Stand zu halten und regelmäßig einen Viren-Scan über alle Laufwerke durchzuführen. Entsprechende Software wird im Rahmen der Campussoftware für Institute der TU zu günstigen Preisen angeboten: sts.tuwien.ac.at/css/.

Wie kommt es zur Wurmverbreitung innerhalb des TUNET?

Trotz TUNET-weiter Sperren auf der TU Firewall für eine Reihe von problematischen Protokollen und Diensten zum Schutze vor einer äußeren Bedrohung, bieten sich noch immer genügend von „innen“ kommende Schlupflöcher, durch die in der Regel aus Unachtsamkeit und Riskovernachlässigung mehr oder wenig fahrlässig Viren oder Würmer ins TUNET gelangen können. Klassische Fälle sind:

- externe Zugänge (Dialin/Modem, WLAN, VPN, Chello StudentConnect, ADSL, xDSL),
- Notebooks, die in „fremden“ Netzen und im TUNET wechselweise betrieben werden,
- Abruf von außerhalb des TUNET gelegenen Mailaccounts (z. B. von Freemail-Providern), ev. in Kombination mit dem Ignorieren von Warnmeldungen lokal installierter Virenwächter.

Welche Schutzmöglichkeiten sind vorhanden bzw. kann man in Anspruch nehmen?

- von außerhalb des TUNET sind typische „gefährliche“ Protokollzugänge/Services (Ports) gesperrt: www.zid.tuwien.ac.at/security/portsperren.php
- von außerhalb des TUNET kann **optional** ein Institutsnetz mit dem Zugriffsschutz versehen werden (alle

Zugänge bis auf definierte IP-Adressen(-Bereiche) und Ports sind gesperrt):

www.zid.tuwien.ac.at/security/zugriffsschutz.php

- von außerhalb und im TUNET kann **optional** das Institutssubnetz mit einer Firewall abgeschottet werden: www.zid.tuwien.ac.at/security/firewall2.php
- von außerhalb und im TUNET samt Institutsnetzwerk schützt **optional** eine Personal Firewall (ev. in Kombination mit einer Anti-Viren-Software), z. B. www.zid.tuwien.ac.at/security/freeware.php#kerio oder entsprechendes Campus-Software Angebot unter: sts.tuwien.ac.at/pss/.

Wichtig in diesem Zusammenhang ist, dass eine Anti-Viren-Software alleine (auch wenn sie am aktuellen Signaturenstand ist) im Normalfall nicht vor einer Wurm-attacke schützt. Hierzu sind Firewall-Maßnahmen bzw. die Beseitigung der entsprechenden Betriebssystemlücken (Einspielen von Sicherheits-Patches) Pflicht.

Eine weitere Kategorie von Plagegeistern ist so genannte Ad- oder Spy-Ware, die zwar von vornherein nicht als gefährlich gelten müssen, aber den Rechnerbetrieb dennoch empfindlich beeinträchtigen (verlangsamten) können und die Privatsphäre durch Aussenden oder Umlenken von Datenströmen aufs Größte verletzen. Diese Klasse von parasitärer Software ist ebenfalls im Normalfall nicht durchgängig von diversen Anti-Viren-Software Paketen in den Griff zu bekommen. Dieser Nische haben sich darauf spezialisierte Programme (z. B. Spybot, Ad-aware) verschrieben.

Definitionen

Ein **Virus** ist ein Programm, das andere Programme „infiltrieren“ kann, indem es sie so modifiziert, dass diese eine möglicherweise mutierte Kopie enthalten.

Ein **Wurm** ist ein Programm, das in der Regel (aber nicht zwingend) einen Viruscharakter aufweist, sich selbst repliziert und verbreitet, ohne ein Wirtsprogramm befallen zu müssen. Der Wurm transferiert sich selbstständig durch das Netzwerk und befällt andere Systeme zu meist auch durch Ausnutzung von Sicherheitslücken.

Unter **Spy-** bzw. **Ad-Ware** versteht man Programme, die dem Verhalten eines Parasiten recht nahe kommen und prinzipiell keinen Schaden anrichten oder eine Verbreitung anstreben, sondern hauptsächlich Informationen aus dem Rechner sammeln und zu fremden Rechnern außerhalb übermitteln bzw. von dort Daten (Werbung) beziehen.

Internet-Service für Studierende: neue Räume und mobiler Zugang

Martin Rathmayer

Das Serviceangebot des ZID wird laufend erweitert und verbessert, um den Studierenden der TU Wien einen optimalen Zugang zu modernen Informationstechnologien zu ermöglichen. Immer mehr Studierende nutzen die frei zugänglichen PC-Arbeitsplätze in den Internet-Räumen, schließen ihre Laptops an die Datentankstellen an und können jetzt auch über WLAN mobil online sein. Im Folgenden werden die neuen Räume und die Bereiche mit mobilem Zugang vorgestellt.

Neue Internet-Räume

Rechtzeitig mit Semesterbeginn wurden drei neue Internet-Räume im Erdgeschoss des neu renovierten Perlmöoserhauses (Operngasse 11) eröffnet. Der Zugang erfolgt entweder direkt durch den Haupteingang in der Operngasse 11 oder durch einen Nebeneingang in der Resselgasse 6, vis-a-vis vom Internet-Raum FH1 im Freihaus. Die drei Räume bieten 35 neue PC-Arbeitsplätze und sollten die Internet-Räume im Freihaus wesentlich entlasten.

Die PCs besitzen 2.4 GHz Pentium-4 Prozessoren, 512 MB Speicher, CDROM, Audio und USB Front-Anschlüsse, optische Wheel-Mäuse und 17" Bildschirme. Im größten Raum (PM1) befindet sich auch ein Drucker. Weiters gibt es 8 Datentankstellen und eine WLAN-Versorgung.



Internet-Raum PM1

Die Raumöffnungszeiten richten sich nach den Gebäude-Öffnungszeiten, d. h. Montag bis Freitag, 7 Uhr bis 19 Uhr 30.

Im Zuge der Umbauarbeiten am Karlsplatz 13, Stiege 7, wird über dem neuen Hörsaal 7 ein weiterer Internet-Raum mit 18 Arbeitsplätzen, 8 Datentankstellen und WLAN errichtet. Die Eröffnung wird voraussichtlich Mitte Dezember erfolgen. Der Raum wird Montag bis Freitag von 7 Uhr 30 bis 19 Uhr geöffnet sein.



Internet-Räume im Bereich Freihaus/Perlmöoserhaus
Lageplan und Zugang

Übersicht Internet-Räume und Datentankstellen


Raum	Adresse	Öffnungszeiten	Rechner	Daten- tankstellen
FH1	Freihaus Wiedner Hauptstraße 8-10 EG, roter Trakt	07:30 bis 21:30 Uhr (Montag bis Freitag, an Vorlesungstagen) 07:30 bis 16:00 (an Samstagen)	37 1 Drucker	8
FH2	Freihaus Wiedner Hauptstraße 8-10 2. OG, gelber Trakt	07:30 bis 21:30 Uhr (Montag bis Freitag, an Vorlesungstagen) kein Betrieb an Samstagen	27 1 Drucker	7
FH3	Freihaus - HTU Fachschaft Physik Wiedner Hauptstraße 8-10 2. OG, gelber Trakt	07:30 bis 21:30 Uhr (Montag bis Freitag, an Vorlesungstagen) kein Betrieb an Samstagen	10	10
FHSR	Schulungsraum Freihaus Wiedner Hauptstraße 8-10 EG, roter Trakt	07:30 bis 21:30 Uhr (Montag bis Freitag, an Vorlesungstagen) kein Betrieb an Samstagen und Ferien	13	-
FHA	Aula Freihaus Wiedner Hauptstraße 8-10 EG, roter Trakt	Siehe Hausöffnungszeiten	5 Igel Terminals	3
BIB	Bibliothek Resselgasse 4, 1. OG	Siehe Öffnungszeiten der Bibliothek	18	40 (je 8 in 1.OG-5.OG)
PM1	Perlmooserhaus Operngasse 11, EG	07:30 bis 19:00 Uhr (Montag bis Freitag) Samstag geschlossen	14 1 Drucker	2
PM2	Perlmooserhaus Operngasse 11, EG	07:30 bis 19:00 Uhr (Montag bis Freitag) Samstag geschlossen	13	-
PM3	Perlmooserhaus Operngasse 11, EG	07:30 bis 19:00 Uhr (Montag bis Freitag) Samstag geschlossen	8	-
PMA	Perlmooserhaus Operngasse 11, EG	07:30 bis 19:00 Uhr (Montag bis Freitag) Samstag geschlossen	-	6
GH	Gußhaus – Altes EI Gußhausstraße 25, 3OG	08:00 bis 21:00 Uhr (Montag bis Freitag, an Vorlesungstagen) Samstag geschlossen	26 1 Drucker	8
GHA	Aula Gußhaus – Neues EI Gußhausstraße 27-29, EG	Siehe Hausöffnungszeiten	8	4
GM	Chemiehochhaus Getreidemarkt 9, 1. UG	07:30 bis 19:00 Uhr (Montag bis Freitag) 07:30 bis 16:00 Uhr (an Samstagen)	19 1 Drucker	6
Bibliothek Chemie	Getreidemarkt 9, 1. OG	Siehe Öffnungszeiten der Bibliothek	-	8
TR	Treitlstraße 3 Hochparterre	07:30 bis 21:30 Uhr (Montag bis Freitag, an Vorlesungstagen) Samstag geschlossen	10	14
BIZ	HTU Bauingenieurzentrum Karlsplatz 13 Stiege 7, 3.OG	08:00 bis 21:00 Uhr (Montag bis Freitag, an Vorlesungstagen) kein Betrieb an Samstagen	10	4
FAV	Favoritenstraße 11, EG	08:00 bis 20:00 Uhr (Montag bis Freitag, an Vorlesungstagen) kein Betrieb an Samstagen	9	-
KP	Karlsplatz 13, Stg. VII	<i>In Bau</i>	(18)	(8)
Nelson's Bar	Paniglgasse 14	Siehe Öffnungszeiten Nelson's Bar	-	10
			222 (240)	130 (138)

Für nächstes Jahr sind weitere Arbeitsplätze im ersten Stock der TU-Bibliothek geplant.

Mobiler Zugang für Studierende

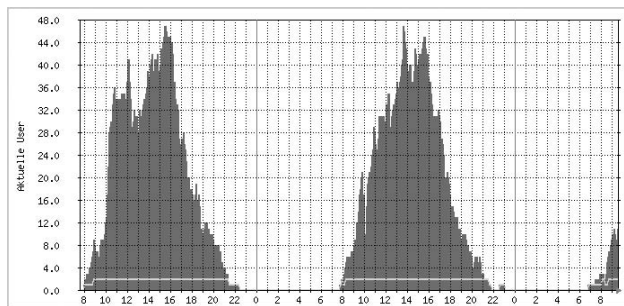
Außer den Internet-Räumen bietet der Zentrale Informatikdienst den Studierenden der TU Wien bereits seit geraumer Zeit einen mobilen Internet-Zugang via Datentankstellen (Notebook-Anschlüsse) und *Wireless* LAN. Die Datentankstellen befinden sich hauptsächlich in den Internet-Räumen, in der TU-Bibliothek und einigen Aula-Bereichen. Die WLAN-Versorgung erstreckt sich zusätzlich noch über einige Hörsäle hinaus.

Datentankstellen

Datentankstellen sind speziell gekennzeichnete  RJ-45 Dosen, die es dem Studenten ermöglichen, mit seinem Notebook ins Internet zu gelangen.

Vorraussetzung dafür ist ein gültiger Studenten-Account. Die technische Realisierung basiert im wesentlichen darauf, dass zuerst per DHCP eine IP-Adresse in einem blinden Netz vergeben wird und danach per PPTP eine Verbindung zum Datentankstellen-Server aufgebaut wird. Die Validierung erfolgt über die Matrikelnummer und das TU-Passwort (vormals White Pages Passwort).

Dose
Daten-
tankstelle



Datentankstellen: Auslastung pro Tag

Das Datentankstellen-Service erfreut sich besonderer Beliebtheit. Seit der Einführung im Jahr 1998 ist jedes Jahr eine Verdoppelung der Benutzer zu beobachten.

Auf Grund der teilweise enormen Auslastung der Internet-Anbindung durch die Datentankstellen wurde ein Limit eingeführt (pro Woche: 5 GB Download, 1 GB Upload; pro Monat: 10 GB Download, 2 GB Upload).

WLAN-Zugang

Bei den Datentankstellen ist der Student räumlich an eine Netzwerk-Dose gebunden, im *Wireless Network* hat er die Möglichkeit, sich innerhalb des Einzugsgebiets der *Access Points* frei zu bewegen. Anders als bei den Datentankstellen erfolgt der Zugang anfänglich zwar auch per DHCP, danach muss sich der Studierende aber nach Aufruf einer beliebigen URL über eine Maske im Webbrowser validieren und wird dann von einem *Universal Subscriber Gateway* für 2 Stunden freigeschaltet. Nach Ablauf dieser Zeit ist eine neuerliche Eingabe der Validierungsdaten erforderlich.

Die Validierung für das WLAN muss gesondert beantragt werden. Da WLAN ein leicht abhörbares Medium darstellt, hat der Studierende zusätzlich die Möglichkeit, nach Installation einer entsprechenden Clientsoftware mit den selben Zugangsdaten seinen Datenverkehr in das TUNET per VPN zu verschlüsseln.

Im WLAN wird derzeit der Standard 802.11b unterstützt. Es ist die Eingabe der SSID *tunet* erforderlich.

Der WLAN-Zugang steht über Antrag auch den Mitarbeitern der TU Wien zur Verfügung.

Der Übersichtsplan auf der nächsten Seite listet alle Standorte mit WLAN-Versorgung auf.

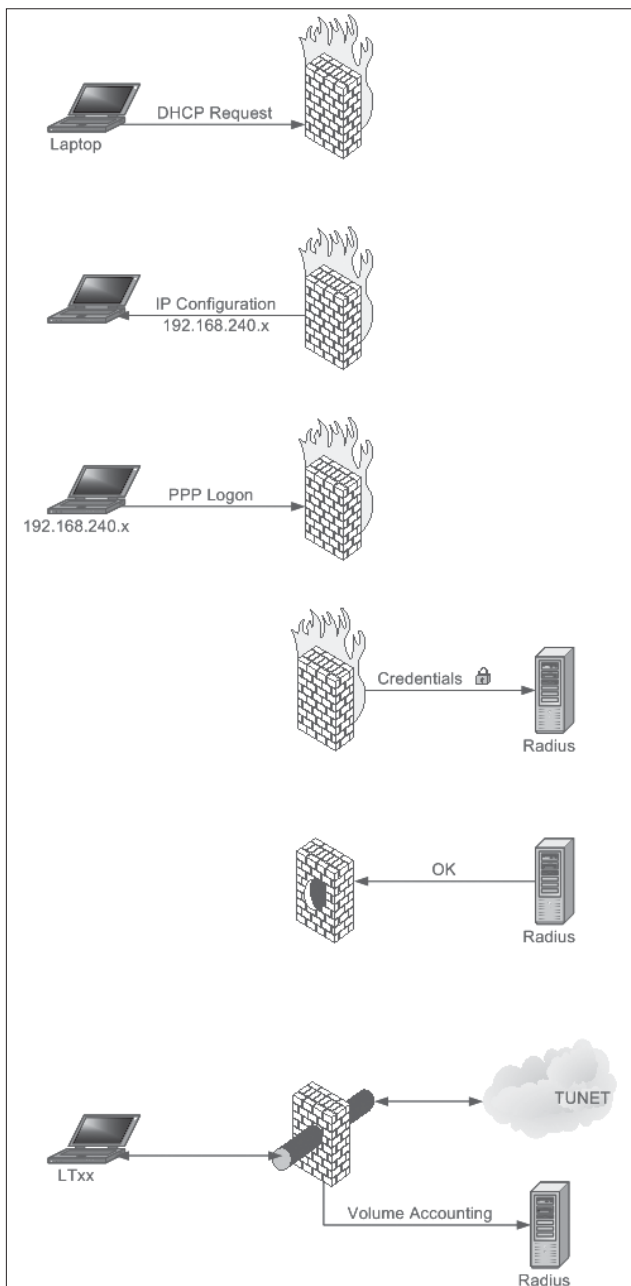
Dank dieser mobilen Zugangsmöglichkeiten und den Internet-Räumen ist jeder Studierende in der Lage, auch während seines Aufenthaltes an der TU Wien jederzeit *online* zu sein.

Weitere Informationen

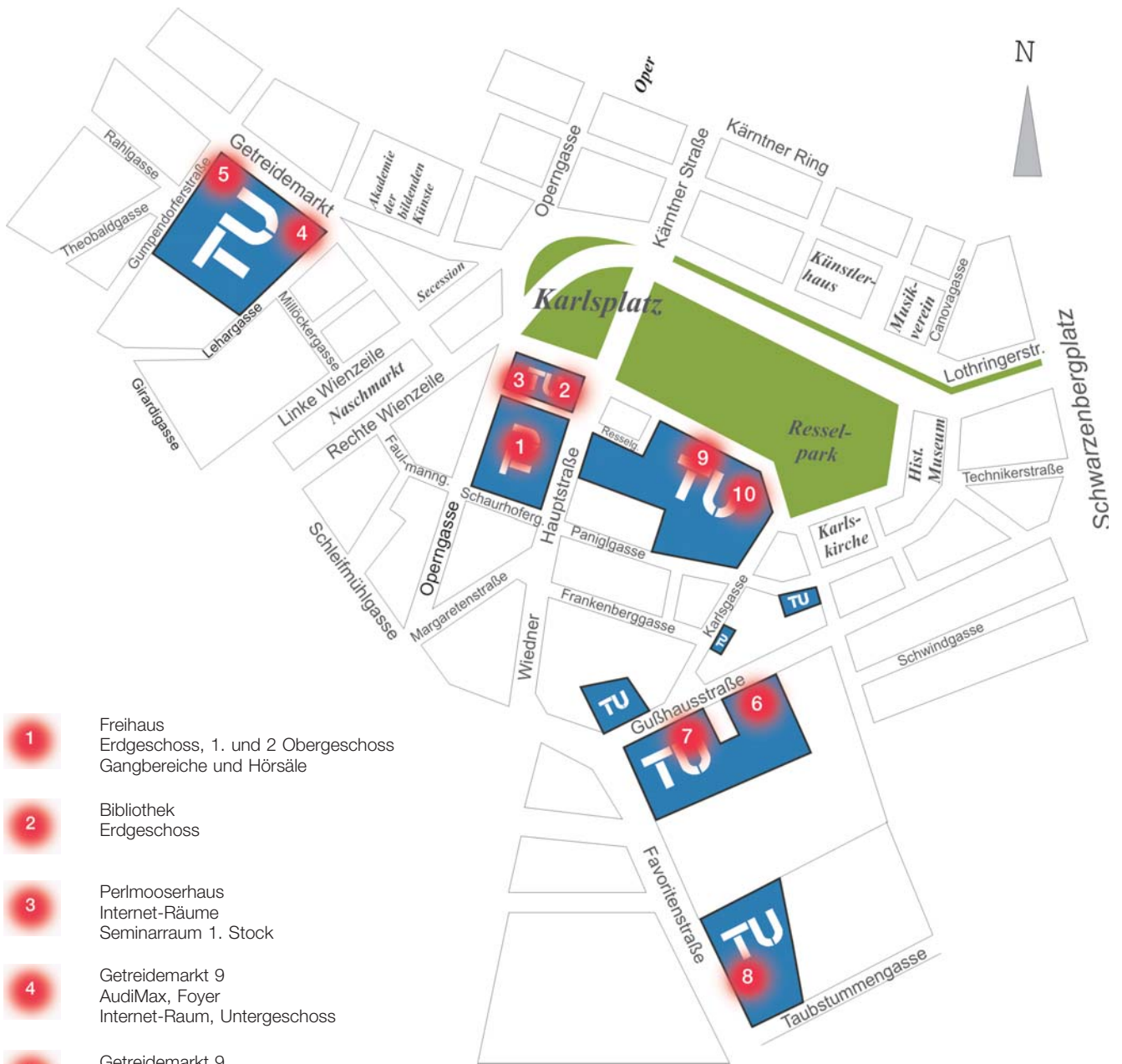
Internet-Service für Studierende: student.tuwien.ac.at

Datentankstellen: student.tuwien.ac.at/datentankstelle/

WLAN an der TU Wien: nic.tuwien.ac.at/tunet/wlan/



Datentankstelle: Verbindungsablauf



WLAN-Versorgung an der TU Wien

Wählleitungen

01 / 589 32
07189 15893

Normaltarif
Online-Tarif
(50 km um Wien)

Datenformate: 300 - 56000 Bit/s (V.92)
MNP5/V.42bis/V.44
PPP
ISDN Synchronous PPP

Auskünfte, Störungsmeldungen

Sekretariat

Tel.: 58801-42001
E-Mail: sekretariat@zid.tuwien.ac.at

Service-Line Abt. Standardsoftware

Tel.: 58801-42004
E-Mail: sekretariat@sts.tuwien.ac.at

TUNET

Störungen

Tel.: 58801-42003
E-Mail: trouble@noc.tuwien.ac.at

Systemunterstützung

Computer Help Line 42124
E-Mail: pss@zid.tuwien.ac.at
Web: sts.tuwien.ac.at/pss/

Rechneranmeldung

E-Mail: hostmaster@noc.tuwien.ac.at

Campussoftware

E-Mail: campus@zid.tuwien.ac.at
gd@zid.tuwien.ac.at

Telekom

Hotline: 08 (nur innerhalb der TU)
E-Mail: telekom@noc.tuwien.ac.at
Chipkarten,
Abrechnung: 58801-42008

Zentrale Server, Operating

Tel.: 58801-42005
E-Mail: operator@zid.tuwien.ac.at

TU-ADSL

Hotline 58801-42007
E-Mail: adslhelp@zid.tuwien.ac.at

Netz- und Systemsicherheit

E-Mail: security@tuwien.ac.at

Internet-Räume

Tel.: 58801-42006
E-Mail: studhelp@zid.tuwien.ac.at

Personalverzeichnis

Telefonliste, E-Mail-Adressen

Zentraler Informatikdienst (ZID)
 der Technischen Universität Wien
 Wiedner Hauptstraße 8-10 / E020
 A - 1040 Wien
 Tel.: (01) 58801-42000 (Leitung)
 Tel.: (01) 58801-42001 (Sekretariat)
 Fax: (01) 58801-42099
 Web: www.zid.tuwien.ac.at

Leiter des Zentralen Informatikdienstes:

W. Kleinert 42010 kleinert@zid.tuwien.ac.at

Administration:

A. Müller 42015 mueller@zid.tuwien.ac.at
 M. Grebhann-Haas 42018 grebhann-haas@zid.tuwien.ac.at

Öffentlichkeitsarbeit

I. Husinsky 42014 husinsky@zid.tuwien.ac.at

Abteilung Zentrale Services

www.zid.tuwien.ac.at/zserv/

Leitung

P. Berger 42070 berger@zid.tuwien.ac.at

W. Altfahrt 42072 altfahrt@zid.tuwien.ac.at
 J. Beiglböck 42071 beiglboeck@zid.tuwien.ac.at
 P. Deinlein 42074 deinlein@zid.tuwien.ac.at
 P. Egler 42094 egler@zid.tuwien.ac.at
 H. Eigenberger 42075 eigenberger@zid.tuwien.ac.at
 C. Felber 42083 felber@zid.tuwien.ac.at
 H. Flamm 42092 flamm@zid.tuwien.ac.at
 W. Haider 42078 haider@zid.tuwien.ac.at
 E. Haunschmid 42080 haunschmid@zid.tuwien.ac.at
 M. Hofbauer 42085 hofbauer@zid.tuwien.ac.at
 P. Kolmann 42095 kolmann@zid.tuwien.ac.at
 F. Mayer 42082 fmayer@zid.tuwien.ac.at
 J. Pfennig 42076 pfennig@zid.tuwien.ac.at
 M. Rathmayer 42086 rathmayer@zid.tuwien.ac.at
 M. Roth 42091 roth@zid.tuwien.ac.at
 J. Sadovsky 42073 sadovsky@zid.tuwien.ac.at
 D. Sonnleitner 42087 sonnleitner@zid.tuwien.ac.at
 E. Srubar 42084 srubar@zid.tuwien.ac.at
 Werner Weiss 42077 weisswer@zid.tuwien.ac.at

Abteilung Kommunikation

nic.tuwien.ac.at

Leitung

J. Demel 42040 demel@zid.tuwien.ac.at
 S. Beer 42061 beer@zid.tuwien.ac.at
 F. Blöser 42041 bloeser@zid.tuwien.ac.at
 G. Bruckner 42046 bruckner@zid.tuwien.ac.at
 A. Datta 42042 datta@zid.tuwien.ac.at
 H. Ehrhardt 42066 ehrhhardt@zid.tuwien.ac.at
 T. Eigner 42052 eigner@zid.tuwien.ac.at
 S. Geringer 42065 geringer@zid.tuwien.ac.at
 T. Gonschorowski 42056 gonschorowski@zid.tuwien.ac.at
 J. Haider 42043 jhaider@zid.tuwien.ac.at
 P. Hasler 42044 hasler@zid.tuwien.ac.at
 H. Kainrath 42045 kainrath@zid.tuwien.ac.at
 J. Klasek 42049 klasek@zid.tuwien.ac.at
 S. Klics 42064 klics@zid.tuwien.ac.at
 W. Koch 42053 koch@zid.tuwien.ac.at
 T. Linneweh 42055 linneweh@zid.tuwien.ac.at
 I. Macsek 42047 macsek@zid.tuwien.ac.at
 M. Markowitsch 42062 markowitsch@zid.tuwien.ac.at
 F. Matasovic 42048 matasovic@zid.tuwien.ac.at
 W. Meyer 42050 meyer@zid.tuwien.ac.at
 R. Vojta 42054 vojta@zid.tuwien.ac.at
 Walter Weiss 42051 weiss@zid.tuwien.ac.at

Abteilung Standardsoftware

sts.tuwien.ac.at

Leitung

A. Blauensteiner 42020 blauensteiner@zid.tuwien.ac.at
 C. Beisteiner 42021 beisteiner@zid.tuwien.ac.at
 J. Donatowicz 42028 donatowicz@zid.tuwien.ac.at
 G. Gollmann 42022 gollmann@zid.tuwien.ac.at
 M. Holzinger 42025 holzinger@zid.tuwien.ac.at
 I. Jaitner 42037 jaitner@zid.tuwien.ac.at
 N. Kamenik 42034 kamenik@zid.tuwien.ac.at
 A. Klauda 42024 klauda@zid.tuwien.ac.at
 H. Mastal 42079 mastal@zid.tuwien.ac.at
 H. Mayer 42027 mayer@zid.tuwien.ac.at
 T. Mikulka 42023 mikulka@zid.tuwien.ac.at
 E. Schörg 42029 schoerg@zid.tuwien.ac.at
 R. Sedlaczek 42030 sedlaczek@zid.tuwien.ac.at
 W. Selos 42031 selos@zid.tuwien.ac.at
 B. Simon 42032 simon@zid.tuwien.ac.at
 A. Sprinzl 42033 sprinzl@zid.tuwien.ac.at
 W. Steinmann 42036 steinmann@zid.tuwien.ac.at
 P. Torzicky 42035 torzicky@zid.tuwien.ac.at